11375 West Sam Houston Parkway South # 800
Houston, Texas 77031

State of Oklahoma, OMES, Central Purchasing

5005 North Lincoln, Suite 300
Oklahoma City, OK 73105

RFP# OK-MA-145, NASPO ValuePoint Master Agreement for Public Safety Video and Vehicle Mounted Equipment

Due Date: July 11, 2016 @ 3:00 p.m. CST/CDT

11375 West Sam Houston Parkway South # 800
Houston, Texas 77031

Date: July 5, 2016

State of Oklahoma, OMES, Central Purchasing
Attn: Lisa Bradley, State Wide Initiatives Contracting Officer
5005 North Lincoln, Suite 300
Oklahoma City, OK 73105

RE: RFP# OK-MA-145, NASPO ValuePoint Master Agreement for Public Safety Video and Vehicle Mounted Equipment

COBAN Technologies, Inc. greatly appreciates the opportunity to respond to the State of Oklahoma OMES Central Purchasing RFP regarding Public Safety Video and Vehicle Mounted Equipment.

COBAN has 14 years of experience providing video evidence capturing and management solutions specifically intended for the law enforcement and first responder industry. Our involvement has offered unique insight into the constantly evolving challenges that agencies face. From equipment to software to support services, COBAN understands the need for a modular, scalable solution that is tailored to fit each department's current and future requirements.

For OMES Central Purchasing, COBAN respectfully presents the COBAN ECHO Body Worn Camera (Band 1), EDGE SD, EDGE Hi-Def, and FUSION HD In-Car Video System (Band 2) solutions for review. The COBAN ECHO BWC (Band 1) EDGE SD, EDGE Hi-Def, and FUSION HD (Band 2) provide features that conform to the department's requirements in an intuitive to operate, reliable, and customizable package. Also, COBAN can provide Local, Cloud, or Hybrid storage solutions in conjunction with our digital video evidence capturing devices.

COBAN also understands that having a solid and robust video management solution is critical for evidence handling. Videos and data captured by our products are managed by our Video Management System software, where features such as access rights, reports, and video retention are all centrally managed. COBAN is able to provide an end-to-end, turnkey solution that is powerful, secure, and streamlined.

COBAN has read and understands all of the terms and conditions as shown in the Master Agreement.

Included in this document is an executive summary, product solutions overview, and brochures for your review. We truly appreciate this opportunity to build a relationship with the Department of Homeland Security. Should you have any questions, please call me at 281-925-0488 Extension #160.

Regards,

Cindy Chang
COBAN Technologies, Inc.
11375 West Sam Houston Parkway South # 800
Houston, Texas 77031
Tel: 281-925-0488 Extension 160
Fax: 281-925-0535
Email: Cindy.Chang@cobantech.com

11375 West Sam Houston Parkway South # 800
Houston, Texas 77031

TABLE OF CONTENTS

- COBAN EDGE SD In-Car Video
- COBAN EDGE Hi-Def In-Car Video
- COBAN FUSION HD In-Car Video
- COBAN Digital Video Management System
- COBAN Command Center
- Digital Property Manager

Section 5

Sample Scope of Work

Key Personnel Resumes

COBAN Business Continuity Plan (Disaster Recovery)

Cloud Standard Terms and Conditions

Microsoft Azure Government Security Documents

COBAN Warranty and Support Statements

11375 West Sam Houston Parkway South # 800
Houston, Texas 77031

SECTION 1

RFP Proposal Forms

- Responding Bidder Form
- Non Collusion Form
- Amendment #1 Acknowledgement
- Amendment #2 Acknowledgement
- Amendment #3 Acknowledgement
- CJIS Agreement
- Past Performance References
- COBAN Proof of Insurance

Responding Bidder Information

*"Certification for Competitive Bid and Contract" **MUST** be submitted along with the response to the Solicitation.*

1. **RE: Solicitation #** OK_MA_145_RFP

2. **Bidder General Information:**

FEI / SSN : 010593612 VEN ID:

Company Name: COBAN Technologies, Inc.

3. **Bidder Contact Information:**

Address: 11375 West Sam Houston Parkway South, #800

City: Houston State: Tx Zip Code: 77031

Contact Name: Cindy Chang

Contact Title: National Sales Support Manager

Phone #: 281-925-0488 ext. 177 FAX#: 281-925-0532

Email: Cindy.Chang@cobantech.com Website: http://www.cobantech.com

4. **Oklahoma Sales Tax Permit[1]:**

☐ YES – Permit #:

☒ NO – Exempt pursuant to Oklahoma Laws or Rules

5. **Registration with the Oklahoma Secretary of State:**

☐ YES - Filing Number:

☒ NO - Prior to the contract award, the successful bidder will be required to register with the Secretary of State or must attach a signed statement that provides specific details supporting the exemption the supplier is claiming (www.sos.ok.gov or 405-521-3911).

6. **Workers' Compensation Insurance Coverage:**

Bidder is required to provide with the bid a certificate of insurance showing proof of compliance with the Oklahoma Workers' Compensation Act.

☒ YES – include a certificate of insurance with the bid

☐ NO - attach a signed statement that provides specific details supporting the exemption you are claiming from the Workers' Compensation Act (Note: Pursuant to Attorney General Opinion #07-8, the exemption from 85 O.S. 2011, § 311 applies only to employers who are natural persons, such as sole proprietors, and does not apply to employers who are entities created by law, including but not limited to corporations, partnerships and limited liability companies.)[2]

Authorized Signature 07-07-2016 Date

Cindy Chang Printed Name

National Sales Support Manager Title

[1] **For frequently asked questions concerning Oklahoma Sales Tax Permit, see http://www.tax.ok.gov/faq/faqbussales.html**

[2] **For frequently asked questions concerning workers' compensation insurance, see http://www.ok.gov/oid/faqs.html#c221**

Certification for Competitive Bid and/or Contract (Non-Collusion Certification)

NOTE: *A certification shall be included with any competitive bid and/or contract exceeding $5,000.00 submitted to the State for goods or services.*

Solicitation or Purchase Order #: OK-MA-145 - Public Safety Video and Vehicle Mounted Equipment

Supplier Legal Name: COBAN Technologies, Inc.

SECTION I [74 O.S. § 85.22]:

A. For purposes of competitive bid,

1. I am the duly authorized agent of the above named bidder submitting the competitive bid herewith, for the purpose of certifying the facts pertaining to the existence of collusion among bidders and between bidders and state officials or employees, as well as facts pertaining to the giving or offering of things of value to government personnel in return for special consideration in the letting of any contract pursuant to said bid;
2. I am fully aware of the facts and circumstances surrounding the making of the bid to which this statement is attached and have been personally and directly involved in the proceedings leading to the submission of such bid; and
3. Neither the bidder nor anyone subject to the bidder's direction or control has been a party:
   a. to any collusion among bidders in restraint of freedom of competition by agreement to bid at a fixed price or to refrain from bidding,
   b. to any collusion with any state official or employee as to quantity, quality or price in the prospective contract, or as to any other terms of such prospective contract, nor
   c. in any discussions between bidders and any state official concerning exchange of money or other thing of value for special consideration in the letting of a contract, nor
   d. to any collusion with any state agency or political subdivision official or employee as to create a sole-source acquisition in contradiction to Section 85.45j.1 of this title.

B. I certify, if awarded the contract, whether competitively bid or not, neither the contractor nor anyone subject to the contractor's direction or control has paid, given or donated or agreed to pay, give or donate to any officer or employee of the State of Oklahoma any money or other thing of value, either directly or indirectly, in procuring this contract herein.

SECTION II [74 O.S. § 85.42]:

For the purpose of a contract for services, the supplier also certifies that no person who has been involved in any manner in the development of this contract while employed by the State of Oklahoma shall be employed by the supplier to fulfill any of the services provided for under said contract.

The undersigned, duly authorized agent for the above named supplier, by signing below acknowledges this certification statement is executed for the purposes of:

☒ **the competitive bid attached herewith and contract, if awarded to said supplier;**

OR

☐ the contract attached herewith, which was not competitively bid and awarded by the agency pursuant to applicable Oklahoma statutes.

Supplier Authorized Signature

07-07-2016
Certified This Date

Cindy Chang
Printed Name

National Sales Support Manager
Title

281-925-0488 ext. 160
Phone Number

Cindy.Chang@cobantech.com
Email

281-925-0535
Fax Number

Amendment of Solicitation

Date of Issuance: May 26, 2016 **Solicitation No.** OK-MA-145

Requisition No. **Amendment No.** 1

Hour and date specified for receipt of offers is changed: ☐ No ☒ Yes, to: July 11, 2016 3:00 PM CST/CDT

Pursuant to OAC 260:115-7-30(d), this document shall serve as official notice of amendment to the Solicitation identified above. Such notice is being provided to all suppliers to which the original solicitation was sent.

Suppliers submitting bids or quotations shall acknowledge receipt of this solicitation amendment prior to the hour and date specified in the solicitation as follows:

(1) Sign and return a copy of this amendment with the solicitation response being submitted; or,

(2) If the supplier has already submitted a response, this acknowledgement must be signed and returned prior to the solicitation deadline. All amendment acknowledgements submitted separately shall have the solicitation number and bid opening date printed clearly on the front of the envelope.

ISSUED BY and RETURN TO:
U.S. Postal Delivery or Personal or Common Carrier Delivery:

Office of Management and Enterprise Services
Central Purchasing
5005 N. Lincoln Blvd., Ste. 300
Oklahoma City, OK 73105

Lisa Bradley
Contracting Officer

405 - 522 - 4480
Phone Number

Lisa.Bradley@omes.ok.gov
E-Mail Address

Description of Amendment:

a. This is to incorporate the following:

1. ****The closing date for this RFP has been extended to July 11, 2016 3:00 PM CDT. ****

2. Attachment D Band 2 has been corrected to reflect correct header and bottom tab information. Updated Attachment has been posted separately.

3. Attachment D Band 4 has removed the siren speaker which has been listed on the market basket. This is currently awarded on a different contract. Updated Attachment has been posted separately.

4. Additional States expressed Intent to Participate

Delaware	Idaho	Illinois
Montana	Nevada	

States which have included terms will have new attachments added.

Attachment M – Illinois
Attachment N – Montana

5. Attachment I has been updated to include the NASPO ValuePoint usage reporting template and has been posted as a separate attachment.

6. Question and Answers:

1. Would a distributor be eligible to submit a bid? (4.1.12)

   a) Will you accept bids from distributors that represent multiple manufacturers that can offer a turn-key solution?

   b) Does this mean you are prohibiting prime bidders that are not manufacturers?

   At this time, we will be accepting proposal responses from manufacturers only. There is opportunity for Authorized Distributors to participate through recommendation from the manufacturer, but all contract awards will be finalized to the manufacturer. See question 79 below.

2. Some products may cross over the defined bands. How would you recommend us to submit these products? *Respondents may incorporate a notation in the product listing to clarify their intention. Such as see Band 3 or an additional comment.*

3. Is the state willing to simplifying price pages? Small/Medium/Large not solution to any size of agency. Good/Better/Best not necessary. *No, the scenarios are set. These do not indicate limits upon which quality the end user may purchase. The examples are to provide suggestions of configurations. Small/medium/large = total suggestion for multiple units integration. Good/better/best for economic choice or all available extras.*

4. Are market basket items applicable to bands 1, 2, 3 or just 4? *The pricing scenarios serve as the general market basket for bands 1, 2, and 3. This allows the supplier to submit their products in areas which apply. These scenarios will be part of the pricing evaluation and it is up to the suppliers to complete the items per category as their offerings.*

5. Since there is only one set of specifications for Band 2, would Attachment D Band 2 have only one price page for completion? *No. Those specifications were set at a minimum standard. We understand that there are base models of equipment as well as models of extra features. The Good Better and Best section is to allow the supplier to provide a variety of products and items for the end users to choose from.*

6. Is it acceptable for Attachment D Band 3 to just have one price page and the vendor can include local and/or cloud storage on that same page? *No. Please reference question #5 above. Both local and*

cloud may be listed on the same page, but there is a differential of good, better, and best level of quality offered.

7. What is definition of Hot List Items? (5.2) *Please reference the term Hot List Items to Market Basket Items.*

8. Where should hot list items be shown on the price pages? *Respondents may also propose additional product identifiers as good, better, or best; contract specific Hot-List Items, as long as pricing will be held for the initial agreement period. These items should be included within the market basket which is contained in each band of Attachment D, pricing cost proposals, and clearly marked as such.*

9. Can Section 4.2.15 be added to the Attachment E Template? *No. Please provide a separate narrative of Section 4.2.15.*

10. Is a point-by-point response in addition to the completed Attachment E required? *Yes.*

11. Section 1.6; please confirm that the States listed will have to have a signed participating addendum in place before they are considered a participating state for this contract? *Yes. A participating addendum will be required for all states which plan on purchasing items from this contract; including the lead state and the states which have signed a non-binding Intent to Participate. Participating Addendums will be executed only after the Master Agreements are awarded.*

12. Is the VPAT reference in Section 9.16 required at the time of bid submission, or is this something that the State will request only when needed? *This will be required during the participating addendum process to reflect each end user's requirements.*

13. Is the vendor required to provide a Certificate of Insurance with the bid response, or after award of contract? If after award, should Certificate of Insurance be provided within 7 days or 30 days of award notification or execution of the Master Agreement?(section 4.18. & 7.17.and ok page 56 bidder info)

Section 4.1.2 Requires Offeror to agree to acquire insurance and this is included with response.
Section 4.1.18 Requires Professional and Technical Insurance be required within 7 days of award notification and sent to the Lead State Contract Administrator.
Section 7.17 Requires submission of Commercial General Liability and any applicable State Workers Compensation or Employers Liability Insurance. These certificates shall be provided within 30 calendar days but prior to any contract performance.

14. In regards to #6 of the "Responding Bidder Information" form, the bidder has no employees in the State of Oklahoma and is not required to maintain Worker's Compensation Insurance in that state. However, all of the bidder's employees are covered by the appropriate Worker's Compensation Insurance in their applicable state of employment. Based on this scenario, should

the bidder mark "yes" or "no" to question #6 on the form? *You should answer yes. Please reference Section 7.17 as this may pertain to each state during the participating addendum process.*

15. In Section 4.1.11 Resume for Account Manager is requested. Is it possible to provide a detailed bio in Attachment E instead of a resume? *No. We would like a full resume of the expected Account Manager.*

16. Section 4.1.17 Disaster Recovery Plan. Is it sufficient that at the time of bid, offeror marks Yes in Attachment E? *No. The evaluation team would like to review all potential awardees disaster recovery plan.*

17. Does the offeror need to specify product delivery / lead time, or will that be provided at the time of quoting the customer? If it is to be specified in bid response, where should the information be located? *A general product delivery/lead time is required with response. A formal delivery date is expected with each individual quotation.*

18. Does offeror provide a response about compliance with minimum requirements or just complete Attachment E "Technical Mandatory" tab? *Offerors must complete Attachment E and include a statement that they have read and understand all of the terms and conditions as shown in Master Agreement (Attachment A)*

19. Whom do we contact if we have questions regarding other states' terms and conditions? *Individual State's terms and conditions will be addressed at time of finalizing the State's Participating Addendum and are not part of the initial Master Agreement or offerors response. These are included as a courtesy to both the State and the offeror.*

20. If our pricing only includes the NASPO Administration Fee will each bidder be responsible for absorbing any additional State Administration Fee? *No. In response offeror should explain that any State Administrative Fees can be added to the baseline pricing.* "*For all such requests, the fee level, payment method and schedule for such reports and payments will be incorporated into the Participating Addendum that is made a part of the Master Agreement. The Contractor may adjust the Master Agreement pricing accordingly for purchases made by Purchasing Entities within the jurisdiction of the state." (7.26.b)*

21. How do we list the Mobile Digital Video products for school buses, mass transit, or other types of non-law enforcement vehicles? *You may include this in Attachment D Band 2 by identifying this in the equipment description. You may consider the Small, Medium, and Large as a volume based solution if applicable.*

22. Please clarify how frequently modifications can be made to this contract for both products and price, during the contract term?

    a) *Discontinued items: 30 day advance notice with substitution information (as needed)*

b) *Marketbasket initial prices and rates must be guaranteed for the first twelve (12) months. After the base year, pricing adjustments may only be submitted quarterly.*

c) *The discount percentage must remain constant for the entire contract term.*

d) *New products can be introduced as applicable. A general guideline is quarterly, however, as a courtesy to the end users, this guideline is flexible.*

23. Please clarify how you want the pricing listed. Turnkey video solution / one complete project / itemized cost breakdown for each component. *Attachment D should list all equipment utilized for a complete project. Equipment should be listed together as a group, but identified with part number and unit cost as the detailed breakdown. These configurations will serve as a sample; however, end users may purchase from full line catalog discount any combination of items at any time.*

24. Will you allow local dealers to provide the integration services? *Any integration services offered should be submitted by the manufacturer through the authorized distributor listing. Listing should list if sales only or sales and service.*

25. How is the State going to integrate this with multiple integrators? *Reference question #23 above.*

26. If Offeror is a manufacturer of equipment in one band but not a manufacture in another band, is Offeror eligible to respond to this RFP to potentially receive an award? *Yes. Awards will be made by bands. You may bid one or all bands as applicable.*

27. May Offeror adjust the width of Column G on Attachment E? *Yes*.

28. Must signatures be original or may they be a scanned copy? *One original signature on the hard master copy is preferable but not a disqualifier.*

29. Please explain why Section 4.1.18 is applicable to the equipment being offered. *Due to the technical and highly confidential nature of this equipment, this insurance will be required.*

30. Can a turn-key License Plate Recognition (LPR) system be accepted by the committee as In-Car Video Equipment under this Band 2? *Yes. A turn-key LPR system on the in-car video contract band would have to meet all the requirements and specifications for the video functionality at a minimum.*

31. May we ask for a waiver of Section 4.1.6 References? No. References are required for your company, and it is understood that this equipment is a new market.

32. Will Section 4.2.15 be added to Attachment E? *No, please address section 4.2.15 as a separate narrative of your marketing and NASPO promotion plan*

33. Section 2.10 – Can the separately sealed and labeled pricing envelope and pricing flash drive be in

the same shipping container as the rest of the response? *Yes, if pricing and flash drive are identified and in a sealed envelope container.*

34. Section 2.11.1 – Are the RFP forms referenced Responding Bidder and Non-Collusion on pages 56 – 57. *Yes.*

35. Section 2.11 – Please clarify where Attachments E, G, and J should be included. *Attachments should be inserted after the technical response.*

36. Section 2.9 – Is Offeror to provide a point by point response to each section of the RFP (pages 1-23), in addition to the content listed in Section 2.11? *Yes*.

37. Do the 5 largest customers need to be contract agreements or customers in general? *Contractual agreement customers would be preferable.*

38. If we have products that have specs in good, better, and best what category should we list the item as? The column where we have the most specifications met? *Not understanding the question. Do not list the same item in all 3 categories.*

39. Under Band 1 requirements there is a record life and a record time specification. Please clarify. *Record life refers to battery life while in active record mode vice standby mode. Record time refers to span or duration of recording on installed storage media; even if you recharge the battery, there is only so much memory.*

40. Unauthorized deletion or alteration. Are we correct in assuming that this is requesting that the unit protects against unauthorized deletion or alteration? ***Yes.***

41. Unauthorized access. Assuming that this is requesting that the unit protects against unauthorized access? *Yes.*

42. Attachment E - Band 3 Are the requirements listed in this section to apply to both a CLOUD based storage solution and a local storage solution? *Yes. This is highly confidential and technical data.*

43. Are vendors able to submit a "range" of storage solutions that fall within a pre-determined price range or are vendors to simply list the amount of percentage off of the storage solution that will be required, once determined? *In the pricing scenarios, a range of storage solutions is allowed. There is a separate tab to list the percentage discount.*

44. Band 3 references peripherals, is this where vendors should list any of the optional items that an agency could elect to purchase in addition to the base units? *Yes, if they remain in the scope and enhance the product. Additionally, options may be listed in the value added section.*

45. Does this also include Wireless equipment and installation services? *It does not include network*

equipment, such as infrastructure, over which the data would travel, such as access points, CAT 5 or 6 wiring, routers, switches, etc. Installation would be limited to the in-car video equipment itself, not generic network infrastructure.

46. In regard to good, better, and best options, are vendors able to list product that is currently in development that will be available for purchase later in the year? If not, what will be the process to get those product lines added to this contract? *Yes with release date information identified.*

47. Are Bands 1 and 2 strictly for the base unit BWC and ICV units or are vendors to list the optional additional items that are available for each band in these sections or in Band 3?

    a) Should integral operating software pricing be included in Band 1 and 2 pricing or should software be priced separately in Band 3 pricing?

Equipment should be listed in the appropriate band, base units in Bands 1 and 2, software /peripherals / hardware / storage solutions should be listed in Band 3. Respondents may include additional sheets providing the full proposed solution.

48. Will the State clarify whether the Master Agreement will be awarded to a single vendor within each cost proposal band, good, better, or best, or if multiple vendors will be selected for the agreement in each category? *There is not anticipated need for a single award per category but the total evaluation points will make the final judgement.*

49. Will the state clarify whether the purchase price discount based on agency size is in regards to the quantity of units purchased or the size of the agency purchasing products? *This is based on the agency purchasing products. We are asking suppliers to propose their solution based on agency size, even though units may be purchased as a single unit.*

50. Regarding Section 2.15.1 Certification for Non-Debarment, does vendor inclusion in an ethics investigation or cancellation of an RFP due to agency accusations of procedural wrong doing warrant "proposed for debarment" or "voluntarily excluded by any Federal, state or local agency? *This certification relates to any legal proceedings which have been made against a supplier which have resulted in a conviction or civil judgement. Cancellation due to agency procedures would not disqualify a supplier. If action is still pending supplier should disclose.*

51. Attachment J Value Added Plan – requires that no identifying information be included. Will the State confirm that value added packages described will be limited to the proposal in which it resides and not extended to all vendors under NASPO? *Attachment J will be evaluated separately and blindly by the evaluation team. Responses will be coded at receipt, and evaluation team will rate the plans without any prior conceptions. This attachment is solely for award from this proposal.*

52. Will the state require vendors to provide a disclaimer on how the BWC mounting solution maintains control over the device during officer struggles? Yes, this is listed in the minimum requirements. *Yes, reference Section 8.4.2.1.*

53. To avoid data loss in critical situations, would the State add a specification to the 'Best' product offering category for vendors to provide details on BWC and In-Car camera automatic activation and the devices required to obtain these features? *These categories are open to allow for the suppliers to identify the areas of quality and extra options of their proposed equipment.*

54. To ensure that NASPO will be able to provide leading technology for an extended period of time, will the State create specifications for real-time communications in the 'Better' product offering (e.g. live streaming), and 'Best' product offering (e.g. visual distribution of dispatch alerts)? *See Question 52 above*

55. To ensure that solutions are comprehensive in CJIS compliance, will the State require vendors to provide a disclaimer regarding how their local storage or removable device storage is CJIS-compliant? *Yes, reference Section 8.6.1.1*.

56. Will the State add a specification to 'Good', 'Better', and 'Best' product offerings in Band 3 including the expected time that will need to be spent by employees to redact a defined amount of video? *No, this contract will not address agency procedures.*

57. How do you expect to reconcile the inherent conflicts when the same products could be available for purchase both in this program and other NASPO programs? *Section 8.6 - Band 3 is not considered to be a hardware category without the purchase of bundled video products and/or accessories.*

58. Based on this Industry Standard, would you please change the term "Authorized Distributors" to "Authorized Resellers"? *No.*

59. Would the State consider the administrative burden you are putting upon manufacturers and change the timeframe for conducting the survey of end users to Bi-annual? (4.2.13) *Yes, the state will agree to bi-annual survey plans.*

60. Section 5.2, par 6: Will the State please define what is meant by the second sentence: "All items must include identifiable baseline references". What is an identifiable baseline reference? And where would be put it on the pricing sheet? *An identifiable baseline reference names where the original pricing originated; such as a catalog or publically available URL. There is space provided on the first tab of each pricing template.*

61. Industry practice is that licenses to use software not transferable. Can the Lead State revise the RFP to state software licenses for storage products are nontransferable unless expressly allowed

by software publisher? *Yes, this language is acceptable. It is also advisable to address this in the participating addendums.*

62. Can the Lead State revise section 4.2.11 to state that products in Band 3 are excluded from the right of return for products ordered in error as this is not a customary practice in the storage industry? *No*.

63. Can the Lead State remove section 4.1.9 as proposers are for-profit entities that must be able to decide on their own whether or not to cancel a product? *No. If awarded a product supplier has a contractual commitment for supplying that product.*

64. Can the Lead State revise section 4.1.17 to read that a vendor shall be prepared to offer a disaster recovery plan if specifically requested and purchased by a customer? *No. Awarded suppliers should address their disaster recovery plan prior to award.*

65. Can the Lead State revise section 5.3.3 to read that offerors may propose their customary terms for cloud services and storage products without being deducted points for excessive exceptions as the RFP does not contain terms for purchasing enterprise information infrastructure products or cloud storage services ? *No, an additional terms where specifics are not mentioned in the RFP are not an exception.*

66. Can the Lead State remove references to the applicable commercial code, as the parties should establish contract terms to govern acceptance? *No. This master agreement is to establish contract terms. Many states have reference to the uniform commercial code in their statutes.*

67. Can the Lead State remove reference to liquidated damages ,latent defects, subsection (1) of 7.14, irrevocable and transfer from sections 7.19 and 7.31, section 7.28 to limit it to inspection of services performed at customer's site, as allowing all customers to inspect a manufacturer's facilities would be highly disruptive? *No. These are standard NASPO ValuePoint terms.*

68. Can the Lead State remove the request for detailed information on the vendors top 5 information as this vendor considers that highly confidential information and does not report that information as part of its public disclosures required by Federal law; instead may a vendor state its overall revenue and its business under 3 SLED contracts? *This is to verify that supplier is qualified to ensure continued support.*

69. Can you please define what is a “local secured storage systems” and "self-contained storage systems" (5.3.3)? Can our response include storage hardware that reside within the agency's data centers? If so, are their specific requirements on size/space/power/cooling/number of sites? Is the vendor or agency employee responsible for administering within agency data center? Can this be done remotely and still comply with the physical separation requirement? *Upon final award*

of the Master Agreements, Awarded Suppliers are able to sign Participating Addendums (PA) at the option of the Participating States. These States reserve the right to add their individual State specific terms and conditions, as well as their own contract management or administrative fee. Each State has it's own IT standards and procedures and will be addressed at the Participating Addendum level

70. .The term Cloud is not defined in government cloud services. Does this mean off premise/hosted? *Yes*

71. Section 4.2.13 - Is the requirement to agree to develop a customer service satisfaction plan or provide the actual plan in the proposal? *Requirement is to agreement to the development and implementation of a customer service satisfaction plan. It is anticipated that this will be a future requirement of an annual supplier meeting.*

72. Is there a designated State retention period for evidential material or is the retention period determined by each jurisdiction? *The resulting master agreements from this solicitation will not attempt to create any policies or procedures.*

73. Is there a designated State retention period for non-evidential material or is the retention period determined by each jurisdiction? *The resulting master agreements from this solicitation will not attempt to create any policies or procedures.*

74. Will the department provide electrical outlets/services and at equipment locations?

Needs will vary depending upon each agency implementation.

Will the department provide network cabling from the department provided network infrastructure to the body worn camera docking equipment location? *Needs will vary depending upon each agency implementation.*

75. Due to the nature and breadth of this RFP, will OK consider allowing a second round of questions to help clarify any additional information based on the first round of questions? *A second round of questions has not been considered.*

76. Will the Lead State allow other States (not currently listed in the RFP) to participate during the life of the contract? And if so how will that be handled amongst awarded vendors? *Yes. After award any State may purchase from the contract by signing a participating addendum with the awarded suppliers of their choice. In addition, counties, cities, municipalities may avail themselves of this contract in many States. It is general NASPO ValuePoint policy for the participating addendum to be signed at the State Government level.*

77. The bid states, "Any product which has been returned for failure of performance.." Can you define how failure of performance will be identified? *Equipment malfunction.*

78. Proposed pricing – pricing fixed for 12 months. Would the State consider a different pricing

model, like cost plus? *No. With the expected accumulated sales and volume, a cost plus model would be not considered.*

79. Section 7.23 Payment – the State wants the ability to use Purchasing Card with no additional charge. Factoring in the administrative fee and the fixed pricing model, Respondent could potentially be under cost for P-card purchases because of the credit card fee. Would the State consider an additional markup for Purchasing Card orders? *No. An additional markup for credit card purchases is not legal in some states. This is a general NASPO ValuePoint term.*

80. We are a Manufacturer, we do not sell direct to end users, and all products sold to our end user are through distribution and through our Authorized Resellers.

a) Will NASPO Value accept our Authorized Resellers to manage our standard credit memos and arrange for return of incorrectly shipped or deficient products?

b) Will NASPO Value accept our Authorized Resellers to manage their standard order/delivery schedules?

c) Will NASPO Valuepoint accept the process where hardware, software, services and warranty quotes are provided by our partners and submitted to our end users?

d) Will NASPO Valuepoint accept our Authorized Resellers receiving end user purchase orders and awards?

All master agreements and contract awards will be made to the manufacturer.

All purchase orders and payments can only be made to the contract awardee.

The business relationship between the manufacturer and their authorized distributors should reflect this business model and should be explained in the initial proposal response.

81. Will NASPO Valuepoint accept Upon Shipment, Contractor shall convey to purchaser good title to the goods free and clear of all liens, pledges, mortgages, encumbrances, or other security interests. *Shipping terms are referenced in Section 7.11*

82. Will NASPO Valuepoint allow a manufacturer to add items that will support the mission to this RFP and enable the best solutions for the bid for Body Cameras, Dash Cameras, Vehicle Equipment, Public Safety, and Law Enforcement? *Yes. Items may be included in the offering as long as they are purchased with the video equipment and not purchased separately. Additional items may also be mentioned in the value added portion.*

83. The spreadsheet where we are to list Authorized Distributors does not have any provisions for limiting the geographic marketing area for a particular area. If we submit the name of an

authorized distributor can we also submit the geographic area where they are authorized to resell our products? *Yes.*

84. Can the prices submitted for items in the market basket be a different percentage discount than the percentage discount being offered for catalog items? *Yes if they are listed as a greater discount and if marketbasket items pricing remains stable for the first initial year after contract award.*

85. This bid is requesting prices where the vendor pays freight. Items in Band 4 like push bumpers and prisoner seats are large and heavy. Since Hawaii is one of the participating states – will there be any consideration of accepting a different vendor-paid-freight price for Hawaii? And how about Alaska if Alaska were to become a participating state in the future? *I would suggest discussions regarding the extra freight during the participating addendum for users outside of the Continental US.*

86. The RFP references attachment C to be completed and signed. Attachment C is a T&C document. Is Section 2, page 8 referring to the Non Collusion Document and Responding Bidder Document as the documents to be completed and signed as part of attachment C? *Yes*.

87. Is the supplier solely responsible for date stamping surveillance data when it is downloaded into the cloud or does supplier have responsibility for coding and cataloguing data for subsequent identification and retrieval? *The supplier is responsible for explaining their equipment's capabilities in this area. There has not been a pre-determined requirement.*

88. Is the supplier responsible for confirming authorization of agencies or persons requesting access to files? *See Question 86 above.*

89. Which parts/sections of the CJIS Security Policy are applicable to Band 3 and what requirements must the bidder on Band 3 expected to meet or something along those lines? *All sections of the CJIS Security Policy should be met for Band 3 items. This shows to be the industry standard in criminal justice/FBI standards.*

90. In section 8.6.1.5 – Are you referencing dedicated cloud storage? Does each agency/State need their own isolated storage or can they all Federal and State customers share one dedicated cloud storage? *This would need to be clarified with each participating addendum negotiation.*

Description of Amendment - continuing

Link to Oklahoma Posting

https://www.ok.gov/dcs/solicit/app/solicitationDetail.php?solID=2369

b. All other terms and conditions remain unchanged.

COBAN Technologies, Inc.		July 06, 2016
Supplier Company Name (**PRINT**)		Date
Cindy Chang	National Sales Support Manager	
Authorized Representative Name (**PRINT**)	Title	Authorized Representative Signature

Amendment of Solicitation

Date of Issuance: June 16, 2016 **Solicitation No.** OK-MA-145

Requisition No. _____ **Amendment No.** 2

Hour and date specified for receipt of offers is changed: ☐ No ☒ Yes, to: July 11, 2016 3:00 PM CST/CDT

Pursuant to OAC 260:115-7-30(d), this document shall serve as official notice of amendment to the Solicitation identified above. Such notice is being provided to all suppliers to which the original solicitation was sent.

Suppliers submitting bids or quotations shall acknowledge receipt of this solicitation amendment prior to the hour and date specified in the solicitation as follows:

(1) Sign and return a copy of this amendment with the solicitation response being submitted; or,

(2) If the supplier has already submitted a response, this acknowledgement must be signed and returned prior to the solicitation deadline. All amendment acknowledgements submitted separately shall have the solicitation number and bid opening date printed clearly on the front of the envelope.

ISSUED BY and RETURN TO:

U.S. Postal Delivery or Personal or Common Carrier Delivery:

Office of Management and Enterprise Services
Central Purchasing
5005 N. Lincoln Blvd., Ste. 300
Oklahoma City, OK 73105

Lisa Bradley
Contracting Officer

405 - 522 - 4480
Phone Number

Lisa.Bradley@omes.ok.gov
E-Mail Address

Description of Amendment:

a. This is to incorporate the following:

1. An additional Intent to Participate was received. States which have expressed interest to date now include:

Delaware	Illinois	Montana	Oklahoma	Virginia
Hawaii	Louisiana	Nevada	Oregon	
Idaho	Mississippi	North Dakota	Utah	

2. Clarification for the executive summary and narrative.

Section 2.11.2 Executive Summary. This is a one or two page executive summary to briefly describe the Offeror's Proposal. The summary should highlight major features of the Proposal. It must also indicate any requirements that cannot be met by the Offeror. The reader should be able to determine the essence of the Proposal by reading the executive Summary.

Section 2.11.3.1 Offeror Narrative. This section references a complete narrative of the offeror's assessment of the work to be performed, (understanding the scope of work), the offerors ability and approach to meet these expectations, and the resources offeror has or will be acquiring to fulfill the requirements. This narrative should demonstrate the offeror's understanding and vision of the desired overall performance expectations.

Description of Amendment - continuing

3. Section 4.1. Mandatory Minimum Administrative Proposal Requirements. The following areas will require a statement of explanation or action plan detail in addition to a yes/no answer.
   4.1.9. Product Availability
   4.1.10. Product Substitutions / Out of Stock Items
   4.1.13. Proposed Pricing
   4.1.14. Time of Order
   4.1.18. Professional/Technical/Special Insurance Requirements.

4. Section 8 – Mandatory Technical Requirements – (each band has additional items to address 8.4.2, 8.5.3, 8.6.1, and 8.7)
   a. Do you provide instruction manuals at no extra cost?
   b. Do you provide installation manuals at no extra cost?
   c. Do you provide training options?
   d. Do you have additional warranties which go beyond the normal market standard?

5. Band 4 - New Section 8.7.1
   a. Proposals should provide a definable breadth of product coverage. Within each category response, it is desired that there are multiple fits for all makes and models of vehicles.
   b. Products submitted with this proposal must be manufactured to meet the quality and standards of Law Enforcement needs.
   c. For prisoner seating items proposed, it shall be required that all seat belts attach or latch at the outside of the vehicle by the door. Seat belts which fasten at the center of vehicle will not be considered due to the potential harm of the officer. Please describe your seat belt positions with your response.
   d. Partitions – Desired products should possess the highest qualities of polycarbonate, acrylic, non-scratching, vertical and/or horizontal sliding, expanded steel or mesh etc. Provide details on the options of partitions and available materials.
   e. Consoles – Does your product carry multiple equipment brands, customizations, faceplates? Please provide details on your options with vehicle consoles.

6. References Section 4.1.6 and 4.2.14
   References are required. It is understood that new products may not have been released or active in the field to have specific references. This request is for references for your company, not specific equipment.

7. Attachment E has been revised and renamed to Attachment E – Revision 2 Administrative and Technical Response Template.xlsx

Description of Amendment - continuing

b. All other terms and conditions remain unchanged.

COBAN Technologies, Inc.	July 06, 2016
Supplier Company Name (**PRINT**)	Date

Cindy Chang	National Sales Support Manager	
Authorized Representative Name (**PRINT**)	Title	Authorized Representative Signature

Amendment of Solicitation

Date of Issuance: July 6, 2016 **Solicitation No.** OK-MA-145

Requisition No. _____ **Amendment No.** 3

Hour and date specified for receipt of offers is changed: ☐ No ☒ Yes, to: July 11, 2016 3:00 PM CST/CDT

Pursuant to OAC 260:115-7-30(d), this document shall serve as official notice of amendment to the Solicitation identified above. Such notice is being provided to all suppliers to which the original solicitation was sent.

Suppliers submitting bids or quotations shall acknowledge receipt of this solicitation amendment prior to the hour and date specified in the solicitation as follows:

(1) Sign and return a copy of this amendment with the solicitation response being submitted; or,

(2) If the supplier has already submitted a response, this acknowledgement must be signed and returned prior to the solicitation deadline. All amendment acknowledgements submitted separately shall have the solicitation number and bid opening date printed clearly on the front of the envelope.

ISSUED BY and RETURN TO:
U.S. Postal Delivery or Personal or Common Carrier Delivery:

Office of Management and Enterprise Services
Central Purchasing
5005 N. Lincoln Blvd., Ste. 300
Oklahoma City, OK 73105

Lisa Bradley
Contracting Officer

405 - 522 - 4480
Phone Number

Lisa.Bradley@omes.ok.gov
E-Mail Address

Description of Amendment:

a. This is to incorporate the following:

This amendment strikes the Attachment D –Cost Proposal - Band 4 Revised052016. An incorrect posting has been made in error.

Please respond with the original Attachment D –Cost Proposal, Band 4.

Question: If a product offers added value, but is listed in the Good, Better, Best Scenario, Can it also be listed separately on Attachment J?

Answer: Yes, if the respondent is offering the product separately and will honor the listed pricing for the initial year after award.

Question: How are we to identify the products on Attachment J, product name or model numbers, or only a description of product and added value they offer?

Answer: The items listed should be clearly identified. Preferably this would include name, model number, description, and the added value they offer.

Description of Amendment - continuing

b. All other terms and conditions remain unchanged.

COBAN Technologies, Inc.		07-06-16
Supplier Company Name (**PRINT**)		Date
Cindy Chang	National Sales Support Manager	
Authorized Representative Name (**PRINT**)	Title	Authorized Representative Signature

FEDERAL BUREAU OF INVESTIGATION

CRIMINAL JUSTICE INFORMATION SERVICES SECURITY ADDENDUM

Legal Authority for and Purpose and Genesis of the Security Addendum

Traditionally, law enforcement and other criminal justice agencies have been responsible for the confidentiality of their information. Accordingly, until mid-1999, the Code of Federal Regulations Title 28, Part 20, subpart C, and the National Crime Information Center (NCIC) policy paper approved December 6, 1982, required that the management and exchange of criminal justice information be performed by a criminal justice agency or, in certain circumstances, by a noncriminal justice agency under the management control of a criminal justice agency.

In light of the increasing desire of governmental agencies to contract with private entities to perform administration of criminal justice functions, the FBI sought and obtained approval from the United States Department of Justice (DOJ) to permit such privatization of traditional law enforcement functions under certain controlled circumstances. In the Federal Register of May 10, 1999, the FBI published a Notice of Proposed Rulemaking, announcing as follows:

> 1. Access to CHRI [Criminal History Record Information] and Related Information, Subject to Appropriate Controls, by a Private Contractor Pursuant to a Specific Agreement with an Authorized Governmental Agency To Perform an Administration of Criminal Justice Function (Privatization). Section 534 of title 28 of the United States Code authorizes the Attorney General to exchange identification, criminal identification, crime, and other records for the official use of authorized officials of the federal government, the states, cities, and penal and other institutions. This statute also provides, however, that such exchanges are subject to cancellation if dissemination is made outside the receiving departments or related agencies. Agencies authorized access to CHRI traditionally have been hesitant to disclose that information, even in furtherance of authorized criminal justice functions, to anyone other than actual agency employees lest such disclosure be viewed as unauthorized. In recent years, however, governmental agencies seeking greater efficiency and economy have become increasingly interested in obtaining support services for the administration of criminal justice from the private sector. With the concurrence of the FBI's Criminal Justice Information Services (CJIS) Advisory Policy Board, the DOJ has concluded that disclosures to private persons and entities providing support services for criminal justice agencies may, when subject to appropriate controls, properly be viewed as permissible disclosures for purposes of compliance with 28 U.S.C. 534.
>
> We are therefore proposing to revise 28 CFR 20.33(a)(7) to provide express authority for such arrangements. The proposed authority is similar to the authority that already exists in 28 CFR 20.21(b)(3) for state and local CHRI systems. Provision of CHRI under this authority would only be permitted pursuant to a specific agreement with an authorized governmental agency for the purpose of providing services for the administration of criminal justice. The agreement would be required to incorporate a security addendum approved

by the Director of the FBI (acting for the Attorney General). The security addendum would specifically authorize access to CHRI, limit the use of the information to the specific purposes for which it is being provided, ensure the security and confidentiality of the information consistent with applicable laws and regulations, provide for sanctions, and contain such other provisions as the Director of the FBI (acting for the Attorney General) may require. The security addendum, buttressed by ongoing audit programs of both the FBI and the sponsoring governmental agency, will provide an appropriate balance between the benefits of privatization, protection of individual privacy interests, and preservation of the security of the FBI's CHRI systems.

The FBI will develop a security addendum to be made available to interested governmental agencies. We anticipate that the security addendum will include physical and personnel security constraints historically required by NCIC security practices and other programmatic requirements, together with personal integrity and electronic security provisions comparable to those in NCIC User Agreements between the FBI and criminal justice agencies, and in existing Management Control Agreements between criminal justice agencies and noncriminal justice governmental entities. The security addendum will make clear that access to CHRI will be limited to those officers and employees of the private contractor or its subcontractor who require the information to properly perform services for the sponsoring governmental agency, and that the service provider may not access, modify, use, or disseminate such information for inconsistent or unauthorized purposes.

Consistent with such intent, Title 28 of the Code of Federal Regulations (C.F.R.) was amended to read:

§ 20.33 Dissemination of criminal history record information.

a) Criminal history record information contained in the Interstate Identification Index (III) System and the Fingerprint Identification Records System (FIRS) may be made available:

1) To criminal justice agencies for criminal justice purposes, which purposes include the screening of employees or applicants for employment hired by criminal justice agencies.

2) To noncriminal justice governmental agencies performing criminal justice dispatching functions or data processing/information services for criminal justice agencies; and

3) To private contractors pursuant to a specific agreement with an agency identified in paragraphs (a)(1) or (a)(6) of this section and for the purpose of providing services for the administration of criminal justice pursuant to that agreement. The agreement must incorporate a security addendum approved by the Attorney General of the United States, which shall specifically authorize access to criminal history record information, limit the use of the information to the purposes for which it is provided, ensure the security and confidentiality of the information consistent with these regulations, provide for sanctions, and contain

such other provisions as the Attorney General may require. The power and authority of the Attorney General hereunder shall be exercised by the FBI Director (or the Director's designee).

This Security Addendum, appended to and incorporated by reference in a government-private sector contract entered into for such purpose, is intended to insure that the benefits of privatization are not attained with any accompanying degradation in the security of the national system of criminal records accessed by the contracting private party. This Security Addendum addresses both concerns for personal integrity and electronic security which have been addressed in previously executed user agreements and management control agreements.

A government agency may privatize functions traditionally performed by criminal justice agencies (or noncriminal justice agencies acting under a management control agreement), subject to the terms of this Security Addendum. If privatized, access by a private contractor's personnel to NCIC data and other CJIS information is restricted to only that necessary to perform the privatized tasks consistent with the government agency's function and the focus of the contract. If privatized the contractor may not access, modify, use or disseminate such data in any manner not expressly authorized by the government agency in consultation with the FBI.

FEDERAL BUREAU OF INVESTIGATION

CRIMINAL JUSTICE INFORMATION SERVICES SECURITY ADDENDUM

The goal of this document is to augment the CJIS Security Policy to ensure adequate security is provided for criminal justice systems while (1) under the control or management of a private entity or (2) connectivity to FBI CJIS Systems has been provided to a private entity (contractor). Adequate security is defined in Office of Management and Budget Circular A- 130 as "security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information."

The intent of this Security Addendum is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

This Security Addendum identifies the duties and responsibilities with respect to the installation and maintenance of adequate internal controls within the contractual relationship so that the security and integrity of the FBI's information resources are not compromised. The security program shall include consideration of personnel security, site security, system security, and data security, and technical security.

The provisions of this Security Addendum apply to all personnel, systems, networks and support facilities supporting and/or acting on behalf of the government agency.

1.0 Definitions

1.01 Contracting Government Agency (CGA) - the government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor subject to this Security Addendum.

1.02 Contractor - a private business, organization or individual which has entered into an agreement for the administration of criminal justice with a Criminal Justice Agency or a Noncriminal Justice Agency.

2.00 Responsibilities of the Contracting Government Agency.

2.01 The CGA will ensure that each Contractor employee receives a copy of the Security Addendum and the CJIS Security Policy and executes an acknowledgment of such receipt and the contents of the Security Addendum. The signed acknowledgments shall remain in the possession of the CGA and available for audit purposes. The acknowledgement may be signed by hand or via digital signature (see glossary for definition of digital signature).

3.0 Responsibilities of the Contractor.

3.01 The Contractor will maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed and all subsequent versions), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

4.00 Security Violations.

4.01 The CGA must report security violations to the CJIS Systems Officer (CSO) and the Director, FBI, along with indications of actions taken by the CGA and Contractor.

4.02 Security violations can justify termination of the appended agreement.

4.03 Upon notification, the FBI reserves the right to:

a. Investigate or decline to investigate any report of unauthorized use;

b. Suspend or terminate access and services, including telecommunications links. The FBI will provide the CSO with timely written notice of the suspension. Access and services will be reinstated only after satisfactory assurances have been provided to the FBI by the CGA and Contractor. Upon termination, the Contractor's records containing CHRI must be deleted or returned to the CGA.

5.00 Audit

5.01 The FBI is authorized to perform a final audit of the Contractor's systems after termination of the Security Addendum.

6.00 Scope and Authority

6.01 This Security Addendum does not confer, grant, or authorize any rights, privileges, or obligations on any persons other than the Contractor, CGA, CJA (where applicable), CSA, and FBI.

6.02 The following documents are incorporated by reference and made part of this agreement: (1) the Security Addendum; (2) the NCIC 2000 Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20. The parties are also subject to applicable federal and state laws and regulations.

6.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they augment the provisions of the CJIS Security Policy to provide a minimum basis for the security of the system and contained information and it is understood that there may be terms and conditions of the appended Agreement which impose more stringent requirements upon the Contractor.

6.04 This Security Addendum may only be modified by the FBI, and may not be modified by the parties to the appended Agreement without the consent of the FBI.

6.05 All notices and correspondence shall be forwarded by First Class mail to:

Information Security Officer

Criminal Justice Information Services Division, FBI 1000 Custer

Hollow Road

Clarksburg, West Virginia 26306

FEDERAL BUREAU OF INVESTIGATION

CRIMINAL JUSTICE INFORMATION SERVICES SECURITY

ADDENDUM

CERTIFICATION

I hereby certify that I am familiar with the contents of (1) the Security Addendum, including its legal authority and purpose; (2) the NCIC Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20, and agree to be bound by their provisions.

I recognize that criminal history record information and related data, by its very nature, is sensitive and has potential for great harm if misused. I acknowledge that access to criminal history record information and related data is therefore limited to the purpose(s) for which a government agency has entered into the contract incorporating this Security Addendum. I understand that misuse of the system by, among other things: accessing it without authorization; accessing it by exceeding authorization; accessing it for an improper purpose; using, disseminating or re-disseminating information received as a result of this contract for a purpose other than that envisioned by the contract, may subject me to administrative and criminal penalties. I understand that accessing the system for an appropriate purpose and then using, disseminating or re-disseminating the information received for another purpose other than execution of the contract also constitutes misuse. I further understand that the occurrence of misuse does not depend upon whether or not I receive additional compensation for such authorized activity. Such exposure for misuse includes, but is not limited to, suspension or loss of employment and prosecution for state and federal crimes.

J. MARK GRIFFIN — 7/7/16

Printed Name/Signature of Contractor Employee — Date

Cindy Chang — July 07, 2016

Printed Name/Signature of Contractor Representative — Date

COBAN Technologies, Inc. National Sales Support Manager

Organization and Title of Contractor Representative

12 ATTACHMENT G – REFERENCE TEMPLATE

Survey Questionnaire – State of Oklahoma

To: Ian Smith
(Name of person completing survey)

Phone: 302-672-5353 Email: Ian.Smith@state.de.us

Subject: Past Performance Survey of: COBAN Technologies, Inc.
(Name of Vendor)

The State of Oklahoma in partnership with NASPO ValuePoint is implementing a process that collects past performance information on firms and their key personnel. The information will be used to assist the State(s) in the selection of firms to perform various projects. The firm/individual listed above has listed you as a client for which they have previously done business.

We would appreciate your taking the time to complete this survey.

Rate each of the criteria on a scale of 1 to 10, with 10 representing that you were very satisfied (and would hire the firm/individual again) and 1 representing that you were very unsatisfied (and would never hire the firm/individual again). Please rate each of the criteria to the best of your knowledge. If you do not have sufficient knowledge of past performance in a particular area, leave it blank.

Once complete, please send the form directly to the Vendor so they may submit the results with their response to our current Request for Proposal.

Client Name: Delaware State Police Completion Date: 8-31-12

Project Name: Digital In-Car Video Solution

NO	CRITERIA	UNIT	
1	How would you rate the supplier's product availability and fill rate?	(1-10)	10
2	How would you rate the experience of the supplier in managing large accounts?	(1-10)	10
3	How would you rate the performance of suppliers products compare to that of its competitors?	(1-10)	8
4	How would rate the suppliers turnaround time when contacted to provide information?	(1-10)	10
5	How would you rate the suppliers ordering system?	(1-10)	10
6	How would you rate the supplier's geographic coverage and ability to deliver throughout all your locations?	(1-10)	10
7	How would you rate supplier's accounts receivable/invoice procedures?	(1-10)	10
8	How would you rate suppliers post sales customer relations (Training, Technical Support, and Assistance)?	(1-10)	10
9	Overall customer satisfaction and comfort level in hiring vendor/individual again	(1-10)	10

Please list any additional comments you may have in the space provided below.

Ian Smith		
Printed Name (of Evaluator)		Signature (of Evaluator)

Thank you for your time and effort in assisting the State of Oklahoma in this important endeavor.

12 ATTACHMENT G – REFERENCE TEMPLATE

Survey Questionnaire – State of Oklahoma

To: Jason Liguori
(Name of person completing survey)

Phone: ~~213-841-9010~~ 213-996-1330 Email: jason.liguori@lapd.lacity.org

Subject: Past Performance Survey of: COBAN Technologies, Inc.
(Name of Vendor)

The State of Oklahoma in partnership with NASPO ValuePoint is implementing a process that collects past performance information on firms and their key personnel. The information will be used to assist the State(s) in the selection of firms to perform various projects. The firm/individual listed above has listed you as a client for which they have previously done business.

We would appreciate your taking the time to complete this survey.

Rate each of the criteria on a scale of 1 to 10, with 10 representing that you were very satisfied (and would hire the firm/individual again) and 1 representing that you were very unsatisfied (and would never hire the firm/individual again). Please rate each of the criteria to the best of your knowledge. If you do not have sufficient knowledge of past performance in a particular area, leave it blank.

Once complete, please send the form directly to the Vendor so they may submit the results with their response to our current Request for Proposal.

Client Name: Los Angeles Police Department Completion Date: Ongoing

Project Name: Digital In-Car Video Solution

NO	CRITERIA	UNIT	
1	How would you rate the supplier's product availability and fill rate?	(1-10)	9
2	How would you rate the experience of the supplier in managing large accounts?	(1-10)	9
3	How would you rate the performance of suppliers products compare to that of its competitors?	(1-10)	10
4	How would rate the suppliers turnaround time when contacted to provide information?	(1-10)	10
5	How would you rate the suppliers ordering system?	(1-10)	—
6	How would you rate the supplier's geographic coverage and ability to deliver throughout all your locations?	(1-10)	9
7	How would you rate supplier's accounts receivable/invoice procedures?	(1-10)	9
8	How would you rate suppliers post sales customer relations (Training, Technical Support, and Assistance)?	(1-10)	10
9	Overall customer satisfaction and comfort level in hiring vendor/individual again	(1-10)	10

Please list any additional comments you may have in the space provided below.

PLEASE SEE ATTACHED FOR ADDITIONAL COMMENTS.

JASON LIGUORI		
Printed Name (of Evaluator)		Signature (of Evaluator)

Thank you for your time and effort in assisting the State of Oklahoma in this important endeavor.

JASON LIGUORI
SERGEANT II

INFORMATION TECHNOLOGY BUREAU

100 West First Street, No. 842
Los Angeles, CA 90012

T 213.996.1330

Jason.Liguori@lapd.lacity.org

www.lapdonline.org

July 6, 2016

To Whom It May Concern,

Coban Technologies Inc. (Coban) has been a Los Angeles Police Department (LAPD) supplier/vendor for more than eight years. During this time, I have had the opportunity to work side-by-side with personnel from Coban as LAPD moved forward with an agency wide implementation of in-car video. Since December 2013, I have been directly responsible for the procurement and installation of the Department's in-car video system. As such, I have first-hand experience working with Coban.

Since the LAPD is actively involved in two separate phases of the in-car video program, I have seen multiple facets of Coban Technologies capabilities. The first is new builds. Coban delivers hundreds of units at once, stages, installs into designated vehicles, tests and verifies the configuration. Coban also sets up back-end servers, configures and tests the system end to end. In this capacity Coban delivers a turn-key system ready for use.

In addition to active build-out, Coban is supporting existing systems currently in use. This requires Coban to supply parts and equipment, provide warranty services, remote diagnostic support and ongoing trouble/issue resolution. Finally, LAPD looks to Coban to provide support in the form of system-wide upgrades and enhancements.

Over the past several years, I have seen Coban's ability to respond to the uncertainties of government funding. Historically, LAPD places large orders of parts and equipment as funding becomes available. I have seen first-hand, Coban's ability to deliver everything from individual parts to hundreds of complete in-car systems on short notice. Shipments arrive carefully packaged, labeled and with minimal breakage/damage. This makes the equipment immediately useable.

Certainly it goes without saying that over a multi-year, long term full system contract there will be issues and challenges. Coban has been a great partner for LAPD through both the inevitable ups and downs of the project. Coban has been very receptive to working within the confines of their contract to deliver the most value to the LAPD.

In summary, on behalf of the Los Angeles Police Department, I strongly encourage the State of Oklahoma to closely look at Coban Technologies, Inc. as a supplier. I am confident that you will find the quality of their products and customer service to be of the highest caliber.

Should you have additional questions or need additional information, please do not hesitate to contact me.

12 ATTACHMENT G – REFERENCE TEMPLATE

Survey Questionnaire – State of Oklahoma

To: Major Miguel Aguilar
(Name of person completing survey)

Phone: 505-827-9068 Email: miguel.aguilar@state.nm.us

Subject: Past Performance Survey of: COBAN Technologies, Inc.
(Name of Vendor)

The State of Oklahoma in partnership with NASPO ValuePoint is implementing a process that collects past performance information on firms and their key personnel. The information will be used to assist the State(s) in the selection of firms to perform various projects. The firm/individual listed above has listed you as a client for which they have previously done business.

We would appreciate your taking the time to complete this survey.

Rate each of the criteria on a scale of 1 to 10, with 10 representing that you were very satisfied (and would hire the firm/individual again) and 1 representing that you were very unsatisfied (and would never hire the firm/individual again). Please rate each of the criteria to the best of your knowledge. If you do not have sufficient knowledge of past performance in a particular area, leave it blank.

Once complete, please send the form directly to the Vendor so they may submit the results with their response to our current Request for Proposal.

Client Name: New Mexico State Police Completion Date: 11-22-13

Project Name: Digital In-Car Video Solution

NO	CRITERIA	UNIT	
1	How would you rate the supplier's product availability and fill rate?	(1-10)	10
2	How would you rate the experience of the supplier in managing large accounts?	(1-10)	10
3	How would you rate the performance of suppliers products compare to that of its competitors?	(1-10)	10
4	How would rate the suppliers turnaround time when contacted to provide information?	(1-10)	9
5	How would you rate the suppliers ordering system?	(1-10)	10
6	How would you rate the supplier's geographic coverage and ability to deliver throughout all your locations?	(1-10)	10
7	How would you rate supplier's accounts receivable/invoice procedures?	(1-10)	10
8	How would you rate suppliers post sales customer relations (Training, Technical Support, and Assistance)?	(1-10)	8
9	Overall customer satisfaction and comfort level in hiring vendor/individual again	(1-10)	10

Please list any additional comments you may have in the space provided below.

We are a rural agency with a challenging install. Coban has worked well with us to ensure the best installation.

Major Miguel Aguilar		
Printed Name (of Evaluator)		Signature (of Evaluator)

Thank you for your time and effort in assisting the State of Oklahoma in this important endeavor.

12 ATTACHMENT G – REFERENCE TEMPLATE

Survey Questionnaire – State of Oklahoma

To: Sgt. Ken Euler
(Name of person completing survey)

Phone: ~~727-420-2784~~ 727-235-4807 Email: keuler@pcsonet.com

Subject: Past Performance Survey of: COBAN Technologies, Inc.
(Name of Vendor)

The State of Oklahoma in partnership with NASPO ValuePoint is implementing a process that collects past performance information on firms and their key personnel. The information will be used to assist the State(s) in the selection of firms to perform various projects. The firm/individual listed above has listed you as a client for which they have previously done business.

We would appreciate your taking the time to complete this survey.

Rate each of the criteria on a scale of 1 to 10, with 10 representing that you were very satisfied (and would hire the firm/individual again) and 1 representing that you were very unsatisfied (and would never hire the firm/individual again). Please rate each of the criteria to the best of your knowledge. If you do not have sufficient knowledge of past performance in a particular area, leave it blank.

Once complete, please send the form directly to the Vendor so they may submit the results with their response to our current Request for Proposal.

Client Name: Pinellas County Sheriffs Office Completion Date: 3-25-16

Project Name: Digital In-Car Video Solution

NO	CRITERIA	UNIT	
1	How would you rate the supplier's product availability and fill rate?	(1-10)	10
2	How would you rate the experience of the supplier in managing large accounts?	(1-10)	10
3	How would you rate the performance of suppliers products compare to that of its competitors?	(1-10)	10
4	How would rate the suppliers turnaround time when contacted to provide information?	(1-10)	10
5	How would you rate the suppliers ordering system?	(1-10)	10
6	How would you rate the supplier's geographic coverage and ability to deliver throughout all your locations?	(1-10)	10
7	How would you rate supplier's accounts receivable/invoice procedures?	(1-10)	10
8	How would you rate suppliers post sales customer relations (Training, Technical Support, and Assistance)?	(1-10)	10
9	Overall customer satisfaction and comfort level in hiring vendor/individual again	(1-10)	10

Please list any additional comments you may have in the space provided below.

All Experiences have been Positive! All Expectations are met and Assistance with technical support is above the rest. Thank You!

Sgt. Kenneth Euler		
Printed Name (of Evaluator)		Signature (of Evaluator)

Thank you for your time and effort in assisting the State of Oklahoma in this important endeavor.

12 ATTACHMENT G – REFERENCE TEMPLATE

Survey Questionnaire – State of Oklahoma

To: Scott Jarmon
(Name of person completing survey)

Phone: 360-596-4921 4902 Email: Scott.Jarmon@wsp.wa.gov

Subject: Past Performance Survey of: COBAN Technologies, Inc.
(Name of Vendor)

The State of Oklahoma in partnership with NASPO ValuePoint is implementing a process that collects past performance information on firms and their key personnel. The information will be used to assist the State(s) in the selection of firms to perform various projects. The firm/individual listed above has listed you as a client for which they have previously done business.

We would appreciate your taking the time to complete this survey.

Rate each of the criteria on a scale of 1 to 10, with 10 representing that you were very satisfied (and would hire the firm/individual again) and 1 representing that you were very unsatisfied (and would never hire the firm/individual again). Please rate each of the criteria to the best of your knowledge. If you do not have sufficient knowledge of past performance in a particular area, leave it blank.

Once complete, please send the form directly to the Vendor so they may submit the results with their response to our current Request for Proposal.

Client Name: Washington State Patrol Completion Date: 7-25-14

Project Name: Digital In-Car Video Solution

Survey Questionnaire – State of Oklahoma

NO	CRITERIA	UNIT	
1	How would you rate the supplier's product availability and fill rate?	(1-10)	9
2	How would you rate the experience of the supplier in managing large accounts?	(1-10)	9
3	How would you rate the performance of suppliers products compare to that of its competitors?	(1-10)	9
4	How would rate the suppliers turnaround time when contacted to provide information?	(1-10)	8
5	How would you rate the suppliers ordering system?	(1-10)	9
6	How would you rate the supplier's geographic coverage and ability to deliver throughout all your locations?	(1-10)	10
7	How would you rate supplier's accounts receivable/invoice procedures?	(1-10)	9
8	How would you rate suppliers post sales customer relations (Training, Technical Support, and Assistance)?	(1-10)	9
9	Overall customer satisfaction and comfort level in hiring vendor/individual again	(1-10)	10

Please list any additional comments you may have in the space provided below.

Scott Jarman		
Printed Name (of Evaluator)		Signature (of Evaluator)

Thank you for your time and effort in assisting the State of Oklahoma in this important endeavor.

CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY): 11/16/2015

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER Arthur J. Gallagher Risk Management Services, Inc. 1900 West Loop South, Suite 1600 Houston TX 77027	**CONTACT NAME:** Sherry Ainsworth **PHONE (A/C, No, Ext):** 713-623-2330 **FAX (A/C, No):** 713-622-6722 **E-MAIL ADDRESS:** sherry_ainsworth@ajg.com
	INSURER(S) AFFORDING COVERAGE — **NAIC #**
	INSURER A : Hartford Casualty Insurance Company — 29424
INSURED COBATEC-02 COBAN Technologies Inc 11375 W Sam Houston Pkwy South, #800 Houston, TX 77010	**INSURER B :** Hartford Fire Insurance Company — 19682 **INSURER C :** Hartford Insurance Company of Illin — 38288 **INSURER D :** **INSURER E :** **INSURER F :**

COVERAGES **CERTIFICATE NUMBER:** 690548096 **REVISION NUMBER:**

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS	
C	X **COMMERCIAL GENERAL LIABILITY** CLAIMS-MADE X OCCUR GEN'L AGGREGATE LIMIT APPLIES PER: X POLICY PRO-JECT LOC OTHER:			61UUNPP6321	11/11/2015	11/11/2016	EACH OCCURRENCE DAMAGE TO RENTED PREMISES (Ea occurrence) MED EXP (Any one person) PERSONAL & ADV INJURY GENERAL AGGREGATE PRODUCTS - COMP/OP AGG	$1,000,000 $300,000 $10,000 $1,000,000 $2,000,000 $2,000,000
C	**AUTOMOBILE LIABILITY** X ANY AUTO ALL OWNED AUTOS SCHEDULED AUTOS HIRED AUTOS NON-OWNED AUTOS			61UUNPP6321	11/11/2015	11/11/2016	COMBINED SINGLE LIMIT (Ea accident) BODILY INJURY (Per person) BODILY INJURY (Per accident) PROPERTY DAMAGE (Per accident)	$1,000,000 $ $ $
A	X **UMBRELLA LIAB** X OCCUR **EXCESS LIAB** CLAIMS-MADE DED X RETENTION $ 10,000			61RHUZE6970	11/11/2015	11/11/2016	EACH OCCURRENCE AGGREGATE	$2,000,000 $2,000,000
B	**WORKERS COMPENSATION AND EMPLOYERS' LIABILITY** Y / N ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? **(Mandatory in NH)** If yes, describe under DESCRIPTION OF OPERATIONS below	N / A		61WEAG2024	11/11/2015	11/11/2016	X PER STATUTE OTH-ER E.L. EACH ACCIDENT E.L. DISEASE - EA EMPLOYEE E.L. DISEASE - POLICY LIMIT	$1,000,000 $1,000,000 $1,000,000
B	Errors & Omissions			61TE027649615	11/11/2015	11/11/2016	each Glitch Limit Aggregate Limit	$2,000,000 $2,000,000

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)

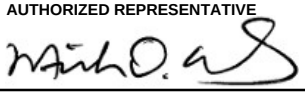
See Attached...

CERTIFICATE HOLDER

CANCELLATION

SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.

AUTHORIZED REPRESENTATIVE



AGENCY CUSTOMER ID: COBATEC-02

LOC #:

ADDITIONAL REMARKS SCHEDULE

AGENCY	NAMED INSURED
Arthur J. Gallagher Risk Management Services, Inc.	COBAN Technologies Inc 11375 W Sam Houston Pkwy South, #800 Houston, TX 77010
POLICY NUMBER	
CARRIER / NAIC CODE	EFFECTIVE DATE:

ADDITIONAL REMARKS

THIS ADDITIONAL REMARKS FORM IS A SCHEDULE TO ACORD FORM,

FORM NUMBER: 25 **FORM TITLE:** CERTIFICATE OF LIABILITY INSURANCE

Blanket Additional Insured with regard to all policies except Workers' Compensation and Errors and Omissions as required by written contract. Blanket Waiver of Subrogation on all polices except Errors & Omissions as required by written contract. Blanket Primary and Non-Contributory with regard to General Liability as required by written contract.

ENDORSEMENTS IF APPLICABLE:
General Liability:
- Blanket Additional Insured as required by written contract HG0001 (06/05)
- Blanket Waiver of Subrogation as required by written contract HG0001 (06/05)
- Blanket Primary and Contributory as required by written contract HG0001 (06/05

Auto Liability:
- Blanket Additional Insured as required by written contract HA9916 (03/12)
- Blanket Waiver of Subrogation as required by written contract HA9916 (03/12)

Workers' Compensation:
- Blanket Waiver of Subrogation as required by written contract WC420304

11375 West Sam Houston Parkway South # 800
Houston, Texas 77031

SECTION 2

COBAN Executive Summary

11375 West Sam Houston Parkway South # 800
Houston, Texas 77031

EXECUTIVE SUMMARY

The following summary introduces COBAN Technologies and how the solution we have proposed will meet the OMES Central Purchasing RFP criteria.

COBAN, was founded in 2002 with the explicit intention of providing comprehensive digital video capture solutions for law enforcement use. Headquartered in Houston, Texas, COBAN has grown to provide over 400 agencies across the United States with a viable, cost-effective means of capturing and maintaining digital media evidence. We serve large agencies such as L.A.P.D., Delaware State Police, Chicago Police Department, Washington State Patrol, and Kansas City PD as well as numerous local agencies across the United States. COBAN pledges to continue our commitment to service and providing scalable solutions for an ever-changing industry.

COBAN Objectives:

To work with OMES Central Purchasing and provide an effective solution to the requests brought forth by this RFP:

- A Body Worn Camera Solution that encompasses the four elements of a turnkey solution: Capture, Transfer, Storage and Management of evidence.
- An In-Car Video Solution that can work with the Body Worn Camera Solution to create a cohesive organization and usage platform.
- A scalable solution that can adapt with the agency's needs.
- Provide a solution that is compatible with the current infrastructure and the possibility of future requirements.
- Maximizing operational efficiency by reducing the amount of time involved with the administration and management of videos, systems, and users involved.

COBAN is aware of the difficulties facing today's law enforcement agencies. In an environment where obligations increase while resources are limited, it is a hard task to balance what is possible with what is necessary. Two major obstacles faced are:

- Budgets
- Infrastructure

Budgets: Funding is, and will always be, the greatest hurdle that agencies face. COBAN will work with any agency under the NASPO ValuePoint Master Agreement in recommending the proper equipment and services that satisfy the project requirements while allowing the flexibility to address changes. We endeavor to always provide the greatest cost-to-performance solutions.

Infrastructure: Although many agencies have an existing IT infrastructure, COBAN would like to extend an open offer to review the multiple network upload and storage options that are available.

We have worked with many agencies, including LAPD, New Mexico State Police, and Chicago Police Department, to create a customized network infrastructure that fit each of their requirements. In no way is this essential to our proposal; if the current infrastructure in place is sufficient to support this project, the COBAN In-Car Video Systems and Body Worn Cameras are compatible.

In-Car Video System Solution:

COBAN is proposing the Integrated EDGE SD, EDGE Hi-Def, and FUSION HD video solutions.

A few of the key features of the EDGE SD In-Car System are:

Cameras:	Front facing SD camera, 18x optical zoom, 48-degree viewing angle
	Rear facing wide-angle IR, 120-degree viewing angle
Video Resolution:	480p front, 600-line rear
Video Format:	MPEG-4
Pre-Event Recording:	Yes, unrestricted and customizable
Post-Event Recording:	Yes, unrestricted and customizable
Storage:	Triple Drive Architecture
	8GB SSD (reserved for OS)
	64GB SSD fix mounted Failsafe
	64GB SSD Removable Mobile Drive
Monitor:	5.7'' Touchscreen, glove operable
Microphones:	900 MHz Wireless transmitter /w two programmable buttons
	Wired Covert in-car
Power Management:	UPS battery /w Smart Power Monitoring, standard
GPS:	Yes
Wi-Fi:	Built-in 802.11 a/g/n/ac
Operating Temperature:	-20°F to +165°F
Durability:	MIL-SPEC 810G certified
Warranty:	3-year standard
	4th and 5th year optional

Please refer to the included Solutions Overview and Brochure for more product information.

A few of the key features of the EDGE Hi-Def In-Car System are:

Cameras:	Front facing HD camera, 28x optical zoom, 12x digital zoom
	55-degree viewing angle
	Optional front facing, low profile panoramic HD camera, 720p
	120-degree viewing angle
	Rear facing wide-angle IR, 120-degree viewing angle
Video Resolution:	720P front, 600-line rear

Video Format:	MPEG-4
Pre-Event Recording:	Yes, unrestricted and customizable
Post-Event Recording:	Yes, unrestricted and customizable
Storage:	Triple Drive Architecture
	8GB SSD (reserved for OS)
	64GB SSD fix mounted Failsafe
	64GB SSD Removable Mobile Drive
Monitor:	5.7'' Touchscreen, glove operable
Microphones:	900 MHz Wireless transmitter /w two programmable buttons
	Wired Covert in-car
Power Management:	UPS battery /w Smart Power Monitoring, standard
GPS:	Yes
Wi-Fi:	Built-in 802.11 a/g/n/ac
Operating Temperature:	-20°F to +165°F
Durability:	MIL-SPEC 810G certified
Warranty:	3-year standard
	4th and 5th year optional

Please refer to the included Solutions Overview and Brochure for more product information.

A few of the key features of the FUSION HD In-Car System are:

Cameras:	Front facing HD Camera, 80-degree viewing angle
	Optional Rear facing wide-angle IR, 120-degree viewing angle
Video Resolution:	720p front, 600-line rear
Video Format:	MP4, H.264 compression
Pre-Event Recording:	Yes, unrestricted and customizable
Post-Event Recording:	Yes, unrestricted and customizable
Storage:	64GB SSD Internal Failsafe
	64GB SSD Removable Pen Drive
Display:	4.3" Touchscreen, glove operable
Microphones:	900 MHz Wireless transmitter /w two programmable buttons
	Wired Covert in-car
Power Management:	UPS battery /w Smart Power Monitoring
GPS:	Yes
Wi-Fi:	Optional module, 802.11 a/g/n
Operating Temperature:	-4°F to +140°F
Durability:	MIL-SPEC 810G certified
Warranty:	1-year standard
	2nd, 3rd, 4th, 5th year optional

Body Worn Camera Solution:

COBAN is proposing the COBAN Integrated ECHO video solution.

A few of the key features of the ECHO Body Worn Camera are:

Dimensions:	3.125" (H) x 2" (W) x 1.06" (D)
Video Resolution:	1080P/720P/D1 configurable
Low Light ability:	Night Mode (0 lux w/IR illuminator)
Pre-Event Recording:	Yes
Angle of View (Main):	110-Degree
Angle of View (POV):	90-Degree
Video Format:	MP4, H.264 compression
Battery Life:	8.5 hours record time @ 720P / 16 hours standby
Internal Storage:	32GB SSD
Buttons:	Record, Flashlight. Tag/Snapshot, and Programmable Multifunction
Connections:	POGO, USB 2.0
IP Rating:	IP56
Camera Positioning:	Modular Clip and POV Clip-on Camera option
Uploading:	6-Bay Upload/Charging Dock
	Single-Bay Upload/Charging Dock (office/vehicle)
	USB Cable
Warranty:	1-year manufacturer warranty standard
	2nd and 3rd year warranty optional

As part of our Body Worn Camera solution, COBAN can also provide a 3-year and 5-year replacement/upgrade plan. At the end of the 2nd year and/or 4th year, the Body Worn Camera in use will be replaced with the latest model of Body Worn Camera from COBAN.

Please refer to the included Solutions Overview and Brochure for more product information.

Integrated with COBAN Video Management System: With all of the In-Car Video systems and Body Worn Cameras, COBAN provides a turnkey Video Management System. Users have the ability to centrally upload and manage all device settings or video retention and export policies under a single application. As part of COBAN Video Management System, access rights and policies can be easily assigned to individuals and groups, certifying that only the proper operators have domain admittance. In addition, the Video Management System is capable of automating many procedures, like generating shift logs, aggregating metadata, and transferring videos to long term storage. While the front end is obviously important, a turnkey solution does not really exist without the ability to easily manage the users, devices, and videos from the back end. Please see the included Solutions Overview for more information regarding COBAN's Video Management System.

Multiple, Scalable Storage Options: The solutions provided by COBAN support Local, Cloud, or Hybrid storage. Because we are aware that storage is not "one-size fits all," COBAN provides departments the flexibility of selecting a solution that will meet the project requirements while still allowing for the possibility of future growth.

A few benefits of Local server based storage are:

- Faster retrieval and access across the network to videos compared to a pure Cloud solution.
- No additional fees for accessing data.
- Connectivity not dependent upon bandwidth.
- Costs are relatively fixed and easier to project over the long term than a pure Cloud solution. Over an extended period of time, Local storage is usually less expensive than Cloud.
- The department has complete control over the maintenance and handling of the data.
- There is no concern about reacquiring archived data at the end of a contract term.

A few benefits of Cloud (remote) based storage are:

- Does not require maintenance of a local server or storage.
- Mitigates the need for dedicated IT personnel.
- Maintenance and security of storage is handled by the SaaS provider.
- Redundancy and disaster recovery is a standard offering.

A few benefits of Hybrid Cloud based storage are:

- Mitigates the need for dedicated IT personnel.
- Allows for faster retrieval and access to certain videos by storing locally while pushing others to the cloud for retention or redundancy.
- Is not as bandwidth intensive as a pure Cloud solution. Less overall network impact than pure Cloud.
- Easier to conform to existing infrastructure capabilities.

Data Security: Security is always a concern when dealing with sensitive and confidential material. COBAN blocks unauthorized traffic to data using a variety of technologies such as firewalls and partitioned Local Area Networks. In addition, all operations, from file access to exporting, are logged to provide a comprehensive audit trail. COBAN also supports authorization based on user role, simplifying access control across defined groups of users. Workstation access to storage and SQL Databases must be explicitly authorized by providing appropriate authorization information to that compute service. The solution provided by COBAN will work in conjunction with an agency's IT personnel to create a secure environment for sensitive data.

Protecting from unauthorized access to data: COBAN's solution involves Network isolation, preventing unwanted tenant-to-tenant communications, while access controls block unauthorized users from the network. Virtual machines do not receive inbound traffic from the Internet unless the agency configures them to do so.

Enhanced digital video solutions: COBAN is currently developing enhanced digital In-Car Video systems and Body Worn Cameras. We are constantly improving our solution based on feedback from the agencies we work with and emerging trends of the industry.

The enhanced ICV, scheduled for release early in 2017, will further the capabilities of COBAN's current digital video systems. Features such as multi-camera 1080p support, multiple HD video and audio channels, on-board hardware encryption, support for IOT architecture, geo-fencing and AVL support, and more will be present. COBAN aims to create a more encompassing and inclusive operation environment by integrating the BWC unit to function with the VMC almost as a single unit. It will build upon the EDGE, FUSION, and ECHO's utility and integration to create a streamlined digital evidence capture ecosystem.

The upcoming BWC will have features like a battery with 13 hours of continuous recording capability and a standby time of more than 24 hours, wireless functionality, mobile app integration, fully customizable pre-event, and more. It will also retain the modularity and configurability of the ECHO, allowing for agencies to operate in accordance to established operating procedures, rather than adjusting policy in order to address limitations. Although these products are not included in the catalog response to OK-MA-145, we feel as if it is important to reiterate COBAN's objective to provide high quality systems implementing the latest technology.

COBAN is a "first-party," end-to-end solutions company. As such, we can provide a complete and efficient project deployment plan. The modularity and scalability of our services enables COBAN to meet many of the challenges associated with deployments. The agencies purchasing under the NASPO ValuePoint Master Agreement can implement a COBAN solution in stages or batches based on funding availability and other factors. We approach each project as a distinct, multi-phase process; tasks of this size require foresight and suitable preparation. We will work closely with every agency choosing the COBAN solution to acquire a real understanding of the situation and the major milestones of the project. From the largest to smallest of agencies, COBAN has provided a personalized and valuable turnkey solution.

11375 West Sam Houston Parkway South # 800
Houston, Texas 77031

SECTION 3

OK-MA-145 Document and Specification Response

Attachment E – Revision 2 Administrative and Technical Response

The State of Oklahoma

OMES Central Purchasing

In conjunction with

NASPO ValuePoint

Request for Proposals

Oklahoma Solicitation Number OK-MA-145

NASPO ValuePoint Master Agreement for Public Safety Video and Vehicle Mounted Equipment

April 20, 2016

REQUEST FOR PROPOSAL
Public Safety / Law Enforcement Video & Vehicle Mounted Equipment

Solicitation # OK-MA-145

1 NASPO VALUEPOINT SOLICITATION - GENERAL INFORMATION

1.1 Purpose

The State of Oklahoma, (Office of Management & Enterprise Services (OMES), Central Purchasing (Lead State) is requesting proposals for Public Safety / Law Enforcement Video & Vehicle Mounted Equipment, in furtherance of the NASPO ValuePoint Cooperative Purchasing Program. The purpose of this Request for Proposal is to establish multiple Master Agreements with qualified offerors that will provide a consistent and reliable source for the provisions of all categories of law enforcement camera systems – in car, body worn, etc. and vehicle mounted equipment which will help law enforcement meet all patrolling needs for all participating states.

The objective of this RFP is to obtain best value, achieve most favorable pricing than is obtainable by an individual state or local government entity because of the collective volume of potential purchases by numerous state and local government entities. The Master Agreement(s) resulting from this procurement may be used by all levels of state governments' i.e. state agencies, local and county government entities, institutions of higher education and other eligible public bodies, the District of Columbia, territories of the United States subject to approval of the individual state procurement director and compliance with local statutory and regulatory provisions.

The initial term of the master agreement shall be 2 (two) years with renewal provisions as outlined in Section 7.3 of the NASPO ValuePoint Master Terms and conditions (Attachment A) which typically extend the original contract period for three (3) additional years.

It is anticipated that this RFP may result in Master Agreement awards to multiple contractors representing the variety of categories, in the Lead State's discretion.

This RFP is designed to provide interested Offerors with sufficient information to submit proposals meeting minimum requirements, but is not intended to limit a proposal's content or exclude any relevant or essential data. Offerors are encouraged to expand upon the specifications to add service and value consistent with state requirements.

While the primary purpose of this solicitation is to select Offerors who can offer the Products or Services for all members participating in the NASPO ValuePoint Cooperative Purchasing Program, Offerors are permitted to submit a Proposal on more limited geographical areas, but not less than one entire Member State. Offerors must clearly describe the geographical limits (e.g. by State name) if proposing a geographical area less than that of all member States. However, if a Offeror elects to submit a Proposal for a single State then the Offeror must be willing to supply the entire State and will not be allowed to add additional States following award or at any time during the term of the contract or any renewals.

The Lead State/Sourcing Team, with the assistance as deemed advisable of the relevant Participating State (or relevant group of Participating States), may evaluate and select a Offeror for

award in more limited geographical areas (e.g. a single state) where judged to be in the best interest of the State or States involved.

1.2 Lead State, Solicitation Number and Lead State Contract Administrator

The State of Oklahoma, Central Purchasing Division is the Lead State and issuing office for this document and all subsequent amendments relating to it. The reference number for the transaction is Solicitation # OK-MA-145. This number must be referred to on all proposals, correspondence, and documentation relating to the RFP.

The Lead State Contract Administrator identified below is the single point of contact during this procurement process. Offerors and interested persons shall direct to the Lead State Contract Administrator all questions concerning the procurement process, technical requirements of this RFP, contractual requirements, requests for brand approval, change, clarification, and protests, the award process, and any other questions that may arise related to this solicitation and the resulting Master Agreement. The Lead State Contract Administrator designated by the State of Oklahoma, Central Purchasing Division is:

Lisa Bradley, State Wide Initiatives Contracting Officer

State of Oklahoma, OMES, Central Purchasing

5005 North Lincoln, Suite 300

Oklahoma City, OK 73105

Lisa.Bradley@omes.ok.gov

405-522-4480 Phone 405-522-1077 Fax

1.3 Schedule of Events (*ANTICIPATED*)

Solicitation Release:	April 20, 2016
Pre-Proposal Conference	May 6, 2016 8:00 AM PT (Pacific Time)
Question Deadline:	May 19, 2016 4:00 PM CDT (Central Daylight Time)
Closing Date and Time:	June 20, 2016 3:00 PM CDT (Central Daylight Time)
Anticipated Award Date:	August 2016

All times is Central Daylight Time Zone (CDT) unless indicated otherwise.

1.4 Definitions

The following definitions apply to this solicitation. Attachment A also contains definitions of terms used in this solicitation and the NASPO ValuePoint Master Agreement terms and conditions.

"Addendum" and its plural **"Addenda"** refer to changes to the contract.

"Amendment(s)" refer to changes made to the original solicitation.

CJIS means Criminal Justice Information Services

Lead State means the State conducting this cooperative procurement, evaluation, and award.

Market basket means a representative sample of items which are being sourced and are directly related to volume or dollar amount activity, and to be used as a baseline for evaluation and/or award purposes.

Offeror means the company or firm who submits a proposal in response to this Request for Proposal.

Proposal means the official written response submitted by an Offeror in response to this Request for Proposal.

"Request for Proposals" or "RFP" means the entire solicitation document, including all parts, sections, exhibits, attachments, and Amendments.

1.5 NASPO ValuePoint Background Information

NASPO ValuePoint (formerly known as WSCA-NASPO) is a cooperative purchasing program of all 50 states, the District of Columbia and the territories of the United States. The Program is facilitated by the NASPO Cooperative Purchasing Organization LLC, a nonprofit subsidiary of the National Association of State Procurement Officials (NASPO), doing business as NASPO ValuePoint. NASPO is a non-profit association dedicated to strengthening the procurement community through education, research, and communication. It is made up of the directors of the central purchasing offices in each of the 50 states, the District of Columbia and the territories of the United States. NASPO ValuePoint facilitates administration of the cooperative group contracting consortium of state chief procurement officials for the benefit of state departments, institutions, agencies, and political subdivisions and other eligible entities (i.e., colleges, school districts, counties, cities, some nonprofit organizations, etc.) for all states, the District of Columbia, and territories of the United States. For more information consult the following websites www.naspo.org **and www.naspovaluepoint.org**

1.6 Participating States

In addition to the Lead State conducting this solicitation, the following Participating States have requested to be named in this RFP as potential users of the resulting Master Agreement: Hawaii, Louisiana, Mississippi, Montana, North Dakota, Utah, and Virginia. Other entities may become Participating Entities after award of the Master Agreement. Some States may have included special or unique terms and conditions for their state that will govern their state Participating Addendum. These terms and conditions are being provided as a courtesy to proposers to indicate which additional terms and conditions may be incorporated into the state Participating Addendum after award of the Master Agreement. The Lead State will not address questions or concerns or negotiate other States' terms and conditions. The participating States will negotiate these terms and conditions directly with the supplier. State-specific terms and conditions are included in Attachments K-L.

1.7 Anticipated Usage

This is a new Master Agreement for the Lead State and NASPO ValuePoint. Therefore, annual usage data is not available. No minimum or maximum level of sales volume is guaranteed or implied in awarded agreements made under this RFP.

2 SOLICITATION REQUIREMENTS, INFORMATION AND INSTRUCTIONS TO OFFERORS

2.1 RFP Question and Answer Process

All questions, including those about Terms and Conditions, must be submitted in writing, to the Lead State Contract Administrator, by May 19, 2016, 4:00 PM CDT, in order to be considered. Written questions must be submitted using Attachment H "Questions & Inquiries Submission Template", and sent via email to the Lead State Contract Administrator. Official answers to all written questions will be posted on the State of Oklahoma's web site as an amendment to the RFP. (https://www.ok.gov/dcs/solicit/app/solicitationSearch.php?status=open-pending) All interested parties may register to receive notification changes by subscribing to the "Notify Me" button posted along with the RFP posting.

The identity of potential Offerors will not be published with the answers, but the text of questions will be restated, so Offeror' s are cautioned about including context in questions that may reveal the source of questions.

2.2 RFP Amendments

Formal changes to this RFP including but not limited to contractual terms and procurement requirements shall only be changed via formal written amendments issued by the Lead State.

The Lead State accepts no responsibility for a prospective Offeror not receiving solicitation documents and/or revisions to the solicitation. It is the responsibility of the prospective Offeror to monitor the State of Oklahoma's website (https://www.ok.gov/dcs/solicit/app/solicitationSearch.php?status=open-pending) to obtain RFP amendments or other information relating to the RFP. It is highly encouraged for each respondent interested in responding to register on this web site. There is a simple "notify me" button, which will alert you to any changes made to the posting.

2.3 Pre-Proposal Conference

A pre-proposal conference will be held on May 6 2016, at (8:00 AM PT), via webinar. Please RSVP this event to Lisa.Bradley@omes.ok.gov; no later than close of business April 29, 2016 to ensure seats as attendance is limited. All suppliers which do RSVP will receive an email invitation to the webinar. Attendance at the conference is not mandatory but is highly recommended. . All interested suppliers should review and be familiar with the scope of this RFP prior to this conference. Questions asked during the pre-proposal conference must also be submitted in writing to the Lead State Contract Administrator for clarification, and answers will be provided via an addendum posted on the Oklahoma web page.

2.4 Proposal Due Date

Proposals must be received by June 20, 2016 3:00 PM CDT. Proposals received after the deadline will be late and ineligible for consideration.

2.5 Cancellation of Procurement

This RFP may be canceled at any time up until the time of award of the Master Agreement(s) if the Lead State determines such action to be in the collective best interests of Participating States.

2.6 Governing Laws and Regulations

This procurement is conducted by the laws of Oklahoma, in accordance with the Oklahoma Central Purchasing Act. This Act is available to view at:
(http://www.ok.gov/DCS/CentralPurchasing/index.html).

Venue for any administrative or judicial action relating to this procurement, evaluation, and award shall be in Oklahoma County, Oklahoma. The provisions governing choice of law and venue for issues arising after award and during contract performance are specified in section 7.35 of the NASPO ValuePoint Master Agreement Terms and Conditions.

2.7 Firm Offers

Responses to this RFP, including proposed costs, will be considered firm for 180 days after the proposal due date.

2.8 Right to Accept All or Portion of Proposal

Unless otherwise specified in the solicitation, the Lead State may accept any item or combination of items as specified in the solicitation or of any proposal unless the Offeror expressly restricts an item or combination of items in its Proposal and conditions any award to receiving all items which was provided in proposal response. In the event that the Offeror so restricts its Proposal, the Lead State may consider the Offeror' s restriction and evaluate whether the award on such basis will result in the best value to the Lead State and the NASPO ValuePoint program. The Lead State may otherwise determine at their sole discretion that such restriction is non-responsive and renders the Offeror ineligible for further evaluation.

2.9 Proposal Content and Format Requirements

Proposals must be detailed and concise. Each Proposal must be labeled and organized in a manner that is congruent with the requirements and terminology used in this RFP and must include a point by point response, structured in form and reference to the RFP, addressing all requirements and the Scope of Work elements.

2.10 Proposal Submission Instructions

Proposals must be received by the posted due date and time. Proposals received after the deadline will be late and ineligible for consideration.

You shall mail or deliver proposal responses to the address listed below on or before the due date and time. .

OMES / Central Purchasing
5005 North Lincoln Boulevard
Suite 300
Oklahoma City, OK 73105

Proposer shall submit one (1) original marked 'MASTER" in hard copy, one (1) redacted copy for public viewing in electronic format, and two (2) electronic copies of the proposal response on a CD ROM or USB flash drive in MS Word 2003 or higher format. (Less Proposal Pricing Page) and all required supporting information and documents on or before the Closing Date and Time.

Envelopes, packages or boxes containing the original and the copies must be clearly labeled and submitted in a sealed envelope, package, or box bearing the following information:

- ☒ Name of Proposer
- ☒ RFP Number
- ☒ Closing Date and Time

If discrepancies are found between the copies, or between the original and copy or copies, the original “MASTER” will provide for the basis of resolving discrepancies. If one document is not clearly marked “MASTER,” Lead State reserves the right to use the original as the Master. If no document can be identified as an original, Proposer’s Proposal may be rejected at the discretion of Lead State.

A Proposer shall submit its Proposal Pricing Page in a separate, sealed envelope, labeled accordingly and placed in sealed carton(s) or package(s) as described above. Prices must be submitted on a pricing matrix Attachment D in Microsoft Excel format. Proposers shall submit their prices in both hard copy and electronic form using Microsoft Excel on a CD-ROM or USB flash drive. Do not include Proposal Pricing Page on the same CD-ROM or USB flash drive as the technical proposal.

Proposers are solely responsible for ensuring that their Proposals are received by Lead State in accordance with the solicitation requirements, before the Closing Date and Time, and at the place specified on the cover sheet of this RFP. Lead State shall not be responsible for any delays in mail or by common carriers or by transmission errors or delays or mistaken delivery. Proposal deliveries made to another location other than to the address identified on the cover sheet of this RFP will be considered non-responsive unless re-delivery is made to the address identified on the cover sheet of this RFP before the Closing Date and Time. Proposals may NOT be submitted by facsimile. All bids submitted shall be subject to the Oklahoma Central Purchasing Act, Central Purchasing Rules, and other statutory regulations as applicable, these General Provisions, any Special Provisions, solicitation specifications, required certification statement, and all other terms and conditions listed or attached herein—all of which are made part of this solicitation.

2.11 Required Format

All Proposals must be submitted in the following format. Detailed information on submitting each of these sections is contained later sections of this RFP.

2.11.1 RFP Forms The Lead State's Request for Proposal forms, reference Attachment C, completed and signed.

2.11.2 Executive Summary The one or two page executive summary is to briefly describe the Offeror's Proposal. This summary should highlight the major features of the Proposal. It must indicate any requirements that cannot be met by the Offeror. The reader should be able to determine the essence of the Proposal by reading the executive summary.

2.11.3 Technical Response This section should constitute the Technical response of the proposal and must contain at least the following information:

2.11.3.1 A complete narrative of the offeror's assessment of the work to be performed, the offerors ability and approach, and the resources necessary to fulfill the requirements. This should demonstrate the offeror's understanding of the desired overall performance expectations. Clearly indicate any options or alternatives proposed.

2.11.3.2 Confidential, Protected or Proprietary Information. All confidential, protected or proprietary Information must be included in this section of proposal response. Do not incorporate protected information throughout the Proposal. Rather, provide a reference in the proposal response directing reader to the specific area of this protected Information section.

2.11.4 Cost Proposal. Cost will be evaluated independently from the technical proposal. Please enumerate all costs on the attached Cost Proposal Form.

The Cost Proposal is to be submitted as a separate document. Inclusion of any cost or pricing data within the technical proposal may result in your Proposal being judged as non-responsive.

2.12 Ownership or Disposition of Proposals and other Materials submitted

Unless otherwise specified in the Oklahoma Open Records Act, Central Purchasing Act, or other applicable law, documents and information a Offeror submits as part of or in connection with a proposal are public records and subject to disclosure.

2.13 Confidential or Proprietary Information

2.13.1 Confidential Information

Proposers should be aware that marking any portion of a Proposal as "confidential", "proprietary" or "trade secret" may exclude it from evaluation or consideration for award. In the event that a limited amount of confidential and proprietary information is deemed necessary by the Offeror to respond to solicitation, any such information must be included in a separate section of the Offeror's proposal response clearly marked as "CONFIDENTIAL AND PROPRIETARY INFORMATION". Do not incorporate confidential and proprietary information throughout the proposal response. Rather, provide a reference in the proposal response directing the reader to the CONFIDENTIAL AND PROPRIETARY INFORMATION section. Elements of the proposal that define the contractual

requirements, such as approaches to the statement of work, prices, and schedule, may not be marked as confidential and proprietary. Proposals not complying with these instructions for identification and segregation of confidential and proprietary information may be rejected.

Information included in the CONFIDENTIAL AND PROPRIETARY INFORMATION section of an Offeror's proposal is not automatically accepted and protected. All information identified in the CONFIDENTIAL AND PROPRIETARY INFORMATION section will be subject to review by the Lead State in accordance with the procedures prescribed by the Lead State's open records statute, freedom of information act, or similar law.

Offeror must identify applicable law supporting their claim of confidentiality. The Oklahoma State Purchasing Director shall make the final decision as to whether the documentation or information is confidential pursuant to 74 O.S. §85.10.

2.13.2 Redacted Proposal Response

In the event that an Offeror includes a CONFIDENTIAL AND PROPRIETARY INFORMATION section in their proposal response, an electronic redacted copy of the offeror's proposal (as accepted) must be submitted with the final proposal (e.g. a best and final offer) or as otherwise directed by the Lead State. Offeror acknowledges that any information in the redacted copy of their proposal response will be made public.

2.14 Offeror Exceptions to Terms and Conditions

The Lead State discourages exceptions to contract terms and conditions in the RFP, attached Participating Entity terms and conditions (if any), and the NASPO ValuePoint Master Agreement Terms and Conditions. Exceptions may cause a proposal to be rejected as nonresponsive when, in the sole judgment of the Lead State (and its evaluation team), the proposal appears to be conditioned on the exception or correction of what is deemed to be a deficiency or unacceptable exception would require a substantial proposal rewrite to correct.

Offerors should identify or seek to clarify any problems with contract language or any other document contained within this RFP through their written inquiries about the RFP using the process in Section 2.1.

Moreover, Offerors are cautioned that award may be made on receipt of initial proposals without clarification or an opportunity for discussion, and the nature of exceptions would be evaluated. Further, the nature of exceptions will be considered in the competitive range determination if one is conducted. Exceptions will be evaluated to determine the extent to which the alternative language or approach poses unreasonable, additional risk to the state, is judged to inhibit achieving the objectives of the RFP, or whose ambiguity makes evaluation difficult and a fair resolution (available to all offerors) impractical given the timeframe for the RFP.

2.15 Certification of Non-Debarment

By submitting a response to this solicitation the prospective primary participant and any other subcontract certifies to the best of their knowledge and belief, that they and their principals or

participants:

2.15.1 Are not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded by any Federal, State or local department or agency;

2.15.2 Have not within a three-year period preceding this proposal been convicted or had a civil judgment rendered against them for commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (Federal, State or local) contract; or for violation of Federal or State antitrust statues or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, or receiving stolen property.

2.15.3 Are not presently indicted for or otherwise criminally or civilly charged by a government entity (Federal, State or local) with commission of any of the offenses listed above this certification; and

2.15.4 Have not with a three-year period preceding this application/proposal had one or more public (Federal, State or local) contracts terminated for cause or default.

RESPONSE: COBAN certifies that we comply with section 2.15 and all the requirements stated in lines 2.15.1 and 2.15.2.

Where the prospective primary participant is unable to certify to any of the statements in this certification, such prospective participant shall attach an explanation to its solicitation response.

3 Evaluation and Award

3.1 Right to Waive Minor Irregularities

The Lead State in its sole discretion reserves the right to waive minor irregularities in the Proposal, which include but are not limited to corrections of deficiencies or clarification of ambiguities that in the judgment of the Lead State do not require a comprehensive proposal rewrite. The Lead State also reserves the right in its sole discretion to waive certain mandatory requirements provided that all of the otherwise responsive proposals fail to meet the same mandatory requirements and the failure to do so does not materially affect the procurement.

3.2 Evaluation Team

A multi-state Sourcing Team will be responsible for the review and evaluation of Proposal in accordance with the process described in the RFP. The Lead State may engage additional qualified individuals during the process to assist the Evaluation Team in understanding technical, financial, legal, contractual, or program matters

3.3 Discussions with Offerors – Oral Presentations

In the initial phase of the evaluation process, the Lead State will review all proposals timely received. Unacceptable proposals (non-responsive proposals not conforming to RFP requirements) will be eliminated from further consideration.

The Lead State reserves the right to award on receipt of initial proposals without an opportunity for discussion or proposal revision, so Offerors are encouraged to submit their most favorable proposal at the time established for receipt of proposals. Offerors shall be accorded fair and equal treatment with respect to any opportunity for discussion and/or written revisions of proposals. In conducting discussions, there shall be no disclosure of any information derived from proposals submitted by competing Offerors.

BEST and FINAL (BAFO): The Lead State may request best and final offers if deemed necessary, and will determine the scope and subject of any best and final request. However, it should not be expected that we will ask for best and final offers to give you an opportunity to strengthen your proposal.

3.4 Award of Master Agreement(s)

Award shall be made to the offeror(s) whose proposal is the most advantageous to Oklahoma and NASPO ValuePoint Participating States, taking into consideration price and the other evaluation factors set forth in this request for proposals. A multiple award is highly anticipated.

The Participating States reserve the right to award items separately or by grouping items, or by total lot.

3.5 Evaluation Process

3.5.1 Phase 1: In the initial phase of the evaluation process, the sourcing team will review all proposals timely received. Non-responsive proposals not conforming to RFP requirements will be eliminated from further consideration.

1. Meets Minimum Mandatory Requirements *Pass/Fail*

3.5.2 Phase 2: Administrative and Technical Proposal Evaluation

Acceptable and potentially acceptable proposals will be evaluated against the proposal evaluation criteria. The Lead State and sourcing team may request clarification from one or more responders. The responses must be made in writing as the Lead State will only use what is in writing for evaluation purposes. The written response to the request for clarification will be combined with the original response, and considered as the amended response. However, the Lead State reserves the right to make an award without further clarification of the responses received. Therefore, it is important that each response be submitted in the most complete manner possible. Responses will be rated as follows:

Evaluation Criteria

Ability to Meet Scope of Work

Administrative Business Response

Technical Response

References

Acceptance of Terms & Conditions

Value Added Plan Response

3.5.3 Phase 3: Cost Proposal Evaluation

Evaluation Criteria

Cost

Evaluation of Cost Proposals: The Offeror with the lowest cost will receive the maximum points. All other Offerors will receive points as determined by the ratio* of their costs to the lowest cost. Final cost scores will be calculated based on the following:

*Ratio Calculation: Points assigned to each Offerors cost proposal will be based on the lowest proposal cost. The Offeror with the lowest proposed cost will receive 100% of the cost points. All other Offerors will receive a portion of the total cost points based on what percentage higher their Proposed Cost is than the Lowest Proposed Cost. Offeror's whose Proposed Cost is more than double (200%) the Lowest Proposed Cost will receive no points. The formula to compute the points is: Cost Points x (2- Proposed Cost/Lowest Proposed Cost).

3.6 Notice of Intent to Award

After a final selection(s) are made, the Lead State, Oklahoma, will issue an intent- to-award announcement on its electronic procurement system. Proposal files are public records and available for review at Lead State by appointment after final award has been made.

3.7 Protest

You may reference the lead state's procedures for a supplier's protest at the following of link provided below.

260:115-3-19. Supplier's Protest

https://www.ok.gov/dcs/searchdocs/app/managedocuments.php?id=946

3.8 Post Award Formalization of the Master Agreement

The Lead State reserves the right during contract negotiation of the Master Agreement to adjust terms and conditions that would not (in the Lead State's judgment) have a material effect on price, schedule, scope of work, or risk to the Lead State and Participating States, with materiality defined in terms of the effect on the evaluation and award. In any event, the Lead State reserves the right to accept contract or pricing changes that are more favorable to the Lead State.

If no Master Agreement is reached with the apparent awardee, the Lead State may negotiate with other Offerors or make no award under this RFP.

4 Administrative and Technical Response Requirements

4.1 Mandatory Minimum Administrative Proposal Requirements

This section contains the minimum requirements that must be met in order to be considered for the evaluation phase. All of the items described in this section are non-negotiable. All Offerors must state willingness and demonstrate ability to satisfy these requirements in the proposal submitted for consideration. Attachment E, Business and Technical Requirements, is provided as a basis for providing your compliance with each section below. There is a yes/no box, and small area for comments. Additional space may be provided if needed.

4.1.1 NASPO ValuePoint Master Agreement Statement of Compliance

NASPO ValuePoint Master Agreement(s) resulting from this RFP will constitute the final agreement except for negotiated terms and conditions specific to a Participating Entity's Participating Addendum.

The Master Agreement will include, but not be limited to, the NASPO ValuePoint Standard Terms and Conditions in Attachment A and Lead State specific terms and conditions required to execute a master agreement, the scope of work Attachment B and selected portions of the Offerors Proposal.

This section highlights particular terms and conditions of NASPO ValuePoint Master Agreement Terms and Conditions, although Offerors will be bound to all the terms and conditions when executing a Master Agreement as shown in Attachment A. Offerors must complete Attachment E, Administrative and Technical Response Template and include a statement in their Proposal that they have read and understand all of the terms and conditions as shown in the Master Agreement (Attachment A).

RESPONSE: COBAN has read and understands the NASPO ValuePoint Master Agreement Statement of Compliance. Please see the signed Attachment A.

4.1.2 Insurance

To be eligible for award, the Offeror agrees to acquire insurance from an insurance carrier or carriers licensed to conduct business in each Participating Entity's state at the prescribed levels set forth in Section 7.17 of the NASPO ValuePoint Master Agreement Terms and Conditions. Describe your insurance or plans to obtain insurance satisfying the requirements in Section 7.17.

RESPONSE: COBAN possesses the necessary Insurance. Please see the attached Proof of Insurance document.

4.1.3 NASPO ValuePoint Administrative Fee and Reporting Requirements

To be eligible for award, the Offeror agrees to pay a NASPO ValuePoint administrative fee as specified in Section 7.26 of the NASPO ValuePoint Master Agreement Terms and Conditions. Moreover, specific summary and detailed usage reporting requirements are prescribed by Section 7.27 of NASPO ValuePoint Master Agreement Terms and Conditions.

Offerors shall identify the person responsible for providing the mandatory usage reports. (This information must be kept current during the contract period) Contractor will be required to provide reporting contact within 15 days of Master Agreement execution.

RESPONSE: COBAN has read and agrees to the NASPO ValuePoint Administrative Fee and Reporting Requirements. The person responsible for providing the mandatory usage reports is Larry Marr.

4.1.4 NASPO ValuePoint eMarket Center

To be eligible for award, the Offeror agrees, by submission of a Proposal, to cooperate with NASPO ValuePoint and SciQuest (and any authorized agent or successor entity to SciQuest) to integrate its presence in the NASPO ValuePoint eMarket Center either through an electronic catalog (hosted or punchout site) or unique ordering instructions. Refer to Attachment A, Section 9, NASPO ValuePoint Master Agreement Terms and Conditions for the prescribed requirements.

Those terms and conditions require as a minimum that the Offeror agree to participate in development of ordering instructions. Proposer shall respond how they can support the eMarket Center in the Proposal through either a hosted catalog or punchout solution.

RESPONSE: COBAN agrees to the terms and requirements set forth by section 4.1.4.

4.1.5 Lead State Terms and Conditions

Refer to Attachment C for the Lead State Special Terms and Conditions that apply to this solicitation and will become part of the Master Agreement Offeror shall indicate in its Proposal that they have read and understand all of the requirements shown Lead State Terms and Conditions and the NASPO ValuePoint Master Agreement Terms and Conditions.

RESPONSE: COBAN has read and understands all of the requirements established by the lead state terms and conditions.

4.1.6 References

Offeror's will provide at least five (5) business references which have purchased similar products in this scope within the last 2 years.

RESPONSE: COBAN has provided the necessary references using the forms provided. Please see the References section of our response.

4.1.7 Participating State Terms and Conditions

As a courtesy to Offerors, some Participating State specific Terms and Conditions are provided in Attachments to this solicitation. These are for informational purposes only and will be negotiated with other Participating States after award of the Master Agreement. Each State reserves the right to negotiate additional terms and conditions in its Participating Addendums. Offerors shall submit a statement that they understand they may be required to negotiate these additional terms and conditions when executing a Participating Addendum.

4.1.8 Quality Assurance and Warranty Guarantee

Offerors should guarantee its products to be free from defects in materials and workmanship, given normal use and care, over a minimum of the standard manufacturer's warranty period, not less than a 12 month period. Offeror should agree to repair and/or immediately replace without charge (including freight both ways) to Authorized Users any product or part thereof that proves to be defective or fails within the warranty period as specified. Please describe your industry standard warranty.

RESPONSE: COBAN agrees to the terms set forth in section 4.1.8. Please see the attached COBAN warranty statements for more information.

4.1.9 Product Availability

The Lead State should not allow any cancellation of products without an equal and acceptable replacement approved by the Contracting Officer. Offerors should communicate discontinuation of any products to the Contracting Officer in writing within five (5) business days. Offerors shall work with the Contracting Officer to identify and implement alternative options that will maintain or reduce costs associated with the replacements. Offerors should offer suggested replacements of discontinued products at least 30 business days prior to substitution, including replacement product number, description, specifications, and final price.

RESPONSE: COBAN agrees to the terms set forth in section 4.1.9.

4.1.10 Emergency Product Substitutions and Out of Stock Items

If necessary to complete a shipment on time, Offeror may request a product substitution. The product substituted should be of equal or better quality and/or grade, at no additional cost, and the Authorized User shall accept the substitution in writing (email is acceptable) prior to delivery. Invoices shall denote all items and quantities as order. Any shorted items shall be noted as “out of stock”.

RESPONSE: COBAN agrees to the terms set forth in section 4.1.10.

4.1.11 Account Manager

The respondent must include the name and professional resume of the individual who will be the

Account Manager for the term of the Contract. The Account Manager will be responsible for operation and administration of the Contract by the Contractor. The Account Manager must respond in a timely manner and in writing unless instructed otherwise, to all information requests from the Contracting Officer.

The Account Manager shall, upon request attend meetings as requested and determined by the Contracting Officer. The Account Manager will be responsible for reports required by the contract and to serve as liaison between the Contractor and Contracting Officer and any other eligible participant. The Contracting Officer may require the Contractor to relieve the Account Manager from work on this contract, if in its opinion, it is apparent that the Account Manager does not deliver work that conforms to performance standards outlined in this RFP. This named Account Manager must be among those present for all scheduled pre-award meetings.

4.1.11.1 Introduce to the Contracting Officer and to the Facilities' staff new products available on the market within the scope of this contract.

4.1.11.2 Maintain and update master price lists/catalogs and review with and distribute to the different Facilities on an ongoing basis.

4.1.11.3 Handle all facility/agency complaints and maintain a log of the complaints and resolutions. Handle all requests from facility/agency/Contracting Officer for inquiries about products.

4.1.11.4 Issue credit memos and arrange for return of incorrectly shipped or deficient products.

4.1.11.5 Resolve any problems and/or discrepancies with the order/delivery schedules.

4.1.11.6 Coordinate with the Contracting Officer any rebate programs or special pricing promotions.

4.1.11.7 Work in conjunction with the Contracting Officer in doing research and making recommendations for product changes to better meet the needs and challenges for all authorized users.

4.1.11.8 Attend annual review meetings as scheduled with Contracting Officer and Sourcing Team.

RESPONSE: COBAN will comply with all of the items listed in section 4.1.11 and all of the corresponding subsections. The Account Manager will be Larry Marr, his Resume is included in the Key Personnel Resumes section.

4.1.12 Authorized Distributors

It is our intent to contract directly with equipment manufacturer (s). As the equipment manufacturer, describe if your products will be provided directly or from authorized distributors. A listing of authorized distributors must be included if applicable.

RESPONSE: COBAN is the manufacturer and distributor of the equipment we sell.

4.1.13 Proposed Pricing

Proposed pricing will remain fixed for the first twelve (12) months of the contract. Requests for additional increases in pricing for contract terms will be limited to once a year. All requests must be made in writing to Contracting Officer a minimum of 30 days prior to request initiation. Documentation justification regarding any increases must be provided. No price increase will be approved without 30 days written notice and written approval from Contracting Officer.

RESPONSE: COBAN has read and agrees to the conditions set forth by section 4.1.13.

4.1.14 Time of Order

If any prices fluctuate between the time of order and delivery, Offeror shall charge the prices in

effect as of the order date.
RESPONSE: COBAN agrees to this requirement.

4.1.15 Additional Fees

Offeror will not invoice services fees or additional costs to the Authorized Users during the term of the contract. There shall be no small order, minimum order, special order, shipping (Except Rush delivery as specified in Attachment D, Pricing) pallet, or fuel charges or surcharges.
RESPONSE: COBAN agrees to the terms set forth in section 4.1.15.

4.1.16 Rebates and Special Offers

Respondents shall offer all rebates and special offers (including commercial and consumer offers) in additional to contracted pricing.
RESPONSE: Please see cost proposal attachments for information.

4.1.17 Disaster Recovery

The State(s) expect the Supplier to have robust disaster recovery capabilities and procedures, to continue service in all aspects of its operations. Supplier shall provide a copy of such plan in response. A more detailed disaster/emergency plan must be completed and approved by the Lead State within thirty (30) days of Contract Award.

In event of a disaster or other emergency at an Authorized User location, Supplier should provide delivery as soon as possible, or within 24 hours after receipt of order to the affected facilities, including weekends, except where Suppliers ability to perform is impaired by same disaster or emergency, in which delivery schedule will be mutually agreed upon.

RESPONSE: Please see the attached COBAN Business Continuity Plan document.

4.1.18 Professional and Technical Special Insurance Requirements

Awarded suppliers will be expected to provide professional and technical, Errors and Omissions, including Network Security and Privacy Liability Insurance, written as a standalone policy or on another form of liability coverage. This policy will provide coverage for all claims the supplier may face legal obligations to pay resulting from any actual or alleged negligent act, error, or omission related to Supplier's professional services required under the contract. Upon award, Supplier is required to carry the following minimum limits:

$2,000,000.00 – per claim or event

$2,000,000.00 – annual aggregate

Any deductible will be the sole responsibility of the Supplier. Date of coverage shall not be after the effective date of this Contract and Offeror shall maintain such insurance for a period of at least three (3) years, following completion of contract. If such insurance is discontinued, extended reporting period coverage must be obtained. Upon notification of award, and within seven (7) days of notification, the awarded vendor(s) must provide a Certificate of Insurance with the coverage and amounts mentioned above. Any contract awarded will not be fully executed until the Certificate of Insurance has been received and approved by the Lead State. The State(s) reserve the right to rescind the contract award if certificate of insurance has not been received within the required time.

RESPONSE: COBAN possesses the necessary Insurance. Please see the attached Proof of Insurance document for more information.

4.2 Desirable Administrative Proposal Requirements

This section contains desirable administrative requirements and will be included in the scorable section of proposal evaluations along with other factors as listed. Attachment E, Business and Technical Requirements, is provided as a basis for providing your compliance with each section below. There is a yes/no box, and small area for comments. Additional pages may be attached if needed.

4.2.1 Response Time

The Awarded Supplier should respond to all communications no later than one business day.
RESPONSE: COBAN will comply with this line item.

4.2.2 Delivery Standards

The Offeror should deliver the products by the delivery date specified on any executed Attachment, Appendix, or Order referencing this Agreement. The Supplier should ensure Delivery Date standards are met no less than 97% of the time.
RESPONSE: COBAN complies with this line item.

4.2.3 Shipping

4.2.3.1 All hazardous materials should be shipped per all Federal and State regulations. The State(s) are committed to recycling and reuse of packaging materials. Some Authorized Users may also require shrink wrapping. Authorized Users will inform Supplier of any such requirements.

RESPONSE: COBAN complies with this line item.

4.2.3.2 All products should be shipped in a matter which enables the receiver to easily check shipment with the invoice. All individual units of measure (cases, rolls, pallets, etc.) should have a clearly visible “vendor product label” containing the following fields:

4.2.3.2.1 Manufacturer Product Number

4.2.3.2.2 Item Description

4.2.3.2.3 Quantity per Unit of Measure

RESPONSE: COBAN complies with this line item.

4.2.4 Freight Policy

All shipments should be F.O.B. Destination to the specified location, with inside delivery if requested. Supplier is responsible for filing and expediting all freight claims with the carrier. The Supplier should pay title and risk of loss or damage charges.
RESPONSE: COBAN complies with this line item.

4.2.5 Invoice Accuracy

Supplier should strive to achieve invoice accuracy of 100% as measured by SKUs ordered.
RESPONSE: COBAN complies with this line item.

4.2.6 Fill Rate

Supplier should maintain a Fill Rate of 98%. The fill rate is calculated for each Authorized User, dividing line items delivered on time by line items ordered during that month and multiplied by 100 to receive percent (%) rate.
RESPONSE: COBAN complies with this line item.

4.2.7 Ordering Methods

Each Authorized User will be responsible for placing its own orders, by written purchase order, telephone, fax, and computer online systems.

4.2.8 Payment Options

Authorized Users will pay the Supplier by check, electronic funds transfer, or the State(s) authorized P-Card (Government credit card).

4.2.9 Invoice Requirements

All invoices should reflect the prices and discounts established for the items on this contract for all orders placed by Authorized Users.

RESPONSE: COBAN complies with this line item.

Before payment is made, Authorized Users will verify that all invoiced charges are correct as per the Contract(s). Only properly submitted invoices will be officially processed for payment. Prompt payment requires that your invoices be accurate, clear, and complete.

4.2.10 Return of Product

4.2.10.1 Any materials delivered in poor condition, in excess of the amount authorized, at the discretion of the Authorized User, will be returned to the Supplier at Supplier's expense within 30 days. Credit for returned goods shall be made immediately upon Suppliers receipt of the returned goods.

4.2.10.2 Any product which has been returned for failure of performance, the Supplier will, at the Authorized Users discretion, refund all amounts paid to the Supplier for product or replace the product.

4.2.10.2.1 Within twenty (20) days of written notification by Authorized User, Supplier should make arrangements for return of the product.

4.2.10.2.2 Supplier should bear all shipping and insurance costs.

4.2.10.2.3 Supplier should be liable for damages to the product, unless caused by fault or negligence of the Authorized User that occur during the return process.

4.2.10.3 Please describe your return policy in detail.

RESPONSE: COBAN agrees to the conditions set forth by section 4.2.10. Please see the attached Sample Scope of Work document and Warranty documents for more information.

4.2.11 Returns Due to User Error

Supplier should provide for return of unopened items ordered in error for up to thirty (30) calendar days from delivery. All returns of unopened items should be provided free-of-charge as long as scheduled at a normal delivery schedule. Otherwise, Authorized Users should be responsible for all costs associated with the preparation and shipment to Suppliers nearest location. No additional charges are allowed, including restocking fees.

RESPONSE: COBAN complies with this line item.

4.2.12 Customer Service

Please provide information relating to the following items regarding your company customer service policy.

4.2.12.1 What are your hours of operation and when are key account people available to us?

RESPONSE: Standard hours of operation are from 7 a.m. to 6 p.m. CST.

4.2.12.2 Describe how problem identification and resolution will be handled.

RESPONSE: Please refer to the attached warranty documents.

4.2.12.3 How do you respond to customer complaints and service issues?

RESPONSE: The customer will be directly contacted by a PMO who handles the account to resolve any complaints or issues. Please refer to the attached warranty documents for more information.

4.2.12.4 How do you assess customer satisfaction?

RESPONSE: The COBAN PMO department will follow up with customers during and after a project deployment to ensure expectations are met and the customer is satisfied.

4.2.12.5 What are your quality assurance measures and how are they handled in your organization.

RESPONSE: Products, both hardware and software, are QA tested in house, on-site at COBAN headquarters in Houston, Texas.

4.2.13 Overall Customer Satisfaction

Offeror should develop a plan to conduct a quarterly survey of end users to determine the level of customer service satisfaction experienced by Authorized Users, and should conduct such a survey upon request from the Contracting Officer. Both the raw and analyzed survey results should be provided to the Contracting Officer. The following includes some of the areas to be measured on the survey: Responsiveness, Communication, Courtesy, Competence, Effectiveness, and Overall Satisfaction.

RESPONSE: COBAN will comply with the terms described in section 4.2.13.

4.2.14 Past Performance References

4.2.14.1 Each Offeror is responsible for sending out the past performance survey questionnaire to at least five (5) past clients which is included as Attachment G – Reference Template.

4.2.14.2 All completed surveys will be submitted with RFP response.

4.2.14.3 Each respondent is responsible for making sure that their past clients receive the survey, complete the survey, and return to them in a timely manner to ensure continuation in the evaluation phase.

4.2.14.4 All returned surveys must be evaluated and signed by the past client. If a survey is not signed, it will not be counted.

4.2.14.5 The State may contact the reference for additional information or to clarify survey data. If the reference cannot be contacted, the survey will be deleted and no credit given for that reference.

4.2.14.6 The scores of the submitted surveys will be used to compile the average past performance rating for each respondent.

RESPONSE: Please see the attached Past Performance References.

4.2.15 Promotion of the NASPO ValuePoint Master Agreement

The NASPO ValuePoint Master Agreement Terms and Conditions include program provisions governing participation in the cooperative, reporting and payment of administrative fees, and marketing/education relating to the NASPO ValuePoint cooperative procurement program. In this regard,

4.2.15.1 Briefly describe how you intend to promote the use of the Master Agreement.

RESPONSE: COBAN will promote the Master Agreement on its website, publications, tradeshows, and talk with potential customers to promote its benefits.

4.2.15.2 Knowing that state procurement officials (CPO) must permit use of the Master Agreement in their state, how will you integrate the CPO's permission into your plan for promoting the agreement?

RESPONSE: COBAN will promote the Master Agreement based on the following benefits:

- **Competitive Pricing – Contracts are established through a competitive solicitation.**
- **Convenient – Significant staff resources, time, and expense can be saved.**
- **Flexible – Contracts are designed to meet the demands and needs of organizations of all sizes.**
- **Transparent – All activities are captured and often published by multiple organizations.**
- **Compliant – Cooperative contracts are designed to meet statutory, policy, and administrative requirements.**

- **Insightful – When using a cooperative approach, the end user has the ability to review and analyze the pricing and services before making a decision to use the contract.**

4.2.15.3 Public entities are sensitive to "scope" issues, that is, whether performance is within the intended scope of the solicitation as awarded. In the context of your method of promoting agreements of this nature, how would you clarify any questions regarding the scope the agreement with respect to any potential order?

RESPONSE: COBAN is providing complete hardware and service offerings to the Master Agreement. Agencies are able to obtain all the solutions and producing offerings from the Master Agreement with minimum gaps.

4.2.15.4 How will your company manage due dates for administrative fee payments and usage reports?

RESPONSE: COBAN's business accounting software will facilitate the administrative fee payment by tracking the origin of the purchase order. If a purchase order is associated with the Master Agreement, the system will flag the transaction, which can be easily tallied during the end-of-month report.

4.2.15.5 Through its Cooperative Development Coordinators and Education & Outreach team, NASPO ValuePoint assists Lead States by engaging vendors in strategies aimed at promoting master agreements. What opportunities and/or challenges do you see in working with NASPO ValuePoint staff in this way?

RESPONSE: COBAN values NASPO's Master Agreement, as it provides a multitude of benefits to the government agencies, such as:

- **Competitive Pricing – Contracts are established through a competitive solicitation.**
- **Convenient – Significant staff resources, time, and expense can be saved.**
- **Flexible – Contracts are designed to meet the demands and needs of organizations of all sizes.**
- **Transparent – All activities are captured and often published by multiple organizations.**
- **Compliant – Cooperative contracts are designed to meet statutory, policy, and administrative requirements.**

- **Insightful – When using a cooperative approach, the end user has the ability to review and analyze the pricing and services before making a decision to use the contract.**

We do not foresee any issues in working with NASPO ValuePoint staff.

5 PRICE AND COST PROPOSAL

Cost in proposals will be evaluated independent of the technical evaluation. Cost proposal must be submitted to the Lead State as a separate document in Offerors Proposal. Do not embed cost proposal in the technical proposal response.

Offeror shall provide detailed pricing for all costs associated with the responsibilities and related services, per Attachment D.

Offer may provide pricing for one band or all bands.

Cost for the NASPO ValuePoint Master Agreements shall be based on the following:

Offeror must submit cost, prices and rates as required by Attachment D Pricing Template. Prices and rates shall include all anticipated charges, including but not limited to, freight and delivery, cost of materials and product, travel expenses, transaction fees, overhead, profits, and other costs or expenses incidental to the Offeror's performance.

The Lead State is exempt from federal excise taxes and no payment will be made for any taxes levied on the Offeror's or any Subcontractor's employee's wages. If required by Lead State, Taxes shall be included as a separate line item on an Offeror's invoice. The tax rules with respect to other Participating Entities may vary and are expected to be addressed in the Participating Addenda. As a general rule, Government Agencies do not pay sales tax.

5.1 Price and Rate Guarantee Period

All prices and rates offered shall be guaranteed for the initial term of the Master Agreement. Any request for price or rate adjustment following the initial Master Agreement term, is detailed in Section 7.6 of the Master Agreement terms and conditions, and must be submitted to Lead State in writing as specified.

5.2 Cost for the NASPO ValuePoint Master Agreements shall be based on the following:

There are four (4) bands of products included with this proposal offering. Each band has a separate pricing template, and is named Attachment D – Band 1, 2, 3, or 4. Respondents may submit pricing for one or all product bands. Additionally, each cost sheet is divided with color tabs at the bottom of each sheet for identification of type of cost required.

To ensure contract flexibility for new technology and product offerings, contract will be awarded at the percentage discount stated per category of item. Clearly indicate how percentage quoted correlates to the identified item description.

Contract pricing shall be marked as a discount percentage from the referenced catalog or publically available URL, and required identified baseline as identified by the item descriptions on pricing tables.

Volume or Cumulative-spend based additional discount percentages are to be clearly marked in tab provided.

Respondents may also propose additional product identifiers as good, better, or best; contract specific Hot-List Items, as long as pricing will be held for the initial agreement period. These items should be included within the market basket which is contained in each band of Attachment D, pricing cost proposals, and clearly marked as such.

Market basket items, unless specifically identified as a special offering, will be used for evaluation purposes. All items must include identifiable baseline references, or will be disqualified from costing evaluation.

5.3 Special pricing instructions per Band

5.3.1 Band 1 (Body Worn Video)

Percentage discounts will outline the basic catalog discount structure. Respondents will identify the baseline used, and category / catalog discounts. The areas for volume discounts and additional discounts are how respondent can show additional incentives.

Cost scenario pricing will be used for evaluation purposes. Each responded shall list proposed product and indicate the category of Good, Better, or Best. Respondent shall indicate if pricing scenario will be offered as a special contract item – specific product line at quoted price.

Offeror is encouraged to provide contract special offerings to entail the final end user's understanding of available body worn video products.

5.3.2 Band 2 (Vehicle Mounted Video – May include Public Transit and School Bus Video/Recording)

Percentage discounts will outline the basic catalog discount structure. Respondents will identify the baseline used, and category / catalog discounts. The areas for volume discounts and additional discounts are how respondent can show additional incentives.

Cost scenario pricing will be used for evaluation purposes. Each respondent shall list proposed product and indicate the category of Good, Better, or Best. Respondent shall indicate if pricing scenario will be offered as a special contract item – specific product line at quoted price.

Offeror is encouraged to provide contract special offerings to entail the final end user's understanding of available vehicle mounted video products

5.3.3 Band 3 (Video Storage, Data Security, Software and Peripherals)

Cost scenarios are provided to allow offeror the ability to provide their best solution for each situation. Offeror may propose multiple storage and security options, and may include both cloud services and secure self-contained storage solutions. These scenarios will be used in evaluation calculations.

Percentage discounts will be used for final award, and must be stated with baseline identified.

Offeror is encouraged to provide contract special offerings to entail the final end user's understanding of available storage and security solutions.

5.3.4 Band 4 (Vehicle Mounted Equipment)

Percentage discounts will outline the basic catalog discount structure. Respondents will identify the baseline used, and category / catalog discounts. The areas for volume discounts and additional discounts are how respondent can show additional incentives.

Percentage discounts will be used for final award, and must be stated with baseline identified.

Marketbasket listed in pricing template will be used for evaluation purposes. Each offeror may bid on one or all categories listed in Band 4. All products listed can be bid as listed or item equivalents, and shall be bid by quantity of one (1) unit of measure. If item does come in multiple pieces, please provide pricing for one complete set or pair and identify unit of measure as such.

Offeror is encouraged to provide contract special offerings to entail the final end user's understanding of available vehicle mounted products.

6 ATTACHMENTS

Attachment A – NASPO Valuepoint Master Agreement Terms and Conditions
Attachment B – Scope of Work
Attachment C – Oklahoma Terms and Conditions for Award
Attachment D – Pricing Templates
Attachment E – Administrative and Technical Response Template
Attachment F – CJIS Security Policy V5.4
Attachment G – Reference Template
Attachment H - Question Template
Attachment I – Reporting Template Example
Attachment J – Value Add Plan Template
Attachment K – Additional State Terms and Conditions (Montana)
Attachment L – Additional State Terms and Conditions (Virginia)

7 ATTACHMENT A: NASPO VALUEPOINT MASTER AGREEMENT TERMS AND CONDITIONS

7.1 Master Agreement Order of Precedence

Any Order placed under this Master Agreement shall consist of the following documents:

(1) Participating Entity's Participating Addendum ("PA");
(2) Oklahoma Terms and Conditions
(3) NASPO ValuePoint Master Agreement Terms & Conditions;
(4) A Purchase Order issued against the Master Agreement;
(5) Attachment B, the Scope of Work;
(6) The Solicitation; and
(7) Contractor's response to the Solicitation, as revised (if permitted) and accepted by the Lead State.

b. These documents shall be read to be consistent and complementary. Any conflict among these documents shall be resolved by giving priority to these documents in the order listed above. Contractor terms and conditions that apply to this Master Agreement are only those that are expressly accepted by the Lead State and must be in writing and attached to this Master Agreement as an Exhibit or Attachment.

7.2 Definitions

Acceptance is defined by the applicable commercial code, except Acceptance shall not occur before the completion of delivery in accordance with the Order, installation if required, and a reasonable time for inspection of the Product.

Contractor means the person or entity delivering Products or performing services under the terms and conditions set forth in this Master Agreement.

Embedded Software means one or more software applications which permanently reside on a computing device.

Intellectual Property means any and all patents, copyrights, service marks, trademarks, trade secrets, trade names, patentable inventions, or other similar proprietary rights, in tangible or intangible form, and all rights, title, and interest therein.

Lead State means the State centrally administering any resulting Master Agreement(s).

Master Agreement means the underlying agreement executed by and between the Lead State, acting on behalf of the NASPO ValuePoint program, and the Contractor, as now or hereafter amended.

NASPO ValuePoint is the NASPO Cooperative Purchasing Organization LLC, doing business as NASPO ValuePoint, a 501(c) (3) limited liability company that is a subsidiary organization the National Association of State Procurement Officials (NASPO), the sole member of NASPO ValuePoint. NASPO ValuePoint facilitates administration of the NASPO cooperative group contracting consortium of state chief procurement officials for the benefit of state departments, institutions, agencies, and political subdivisions and other eligible entities (i.e., colleges, school districts, counties, cities, some nonprofit organizations, etc.) for all states and the District of Columbia. NASPO ValuePoint is identified in the Master Agreement as the recipient of reports and may perform contract administration functions relating to collecting and receiving reports as well as other contract administration functions as assigned by the Lead State.

Order or Purchase Order means any purchase order, sales order, contract or other document used by a Purchasing Entity to order the Products.

Participating Addendum means a bilateral agreement executed by a Contractor and a Participating Entity incorporating this Master Agreement and any other additional Participating Entity specific language or other requirements, e.g. ordering procedures specific to the Participating Entity, other terms and conditions.

Participating Entity means a state, or other legal entity, properly authorized to enter into a Participating Addendum.

Participating State means a state, the District of Columbia, or one of the territories of the United States that is listed in the Request for Proposal as intending to participate. A Participating State is not required to participate through execution of a Participating Addendum. Upon execution of the Participating Addendum, a Participating State becomes a Participating Entity; however, a Participating State listed in the Request for Proposals is not required to participate through execution of a Participating Addendum.

Product means any equipment, software (including embedded software), documentation, service or other deliverable supplied or created by the Contractor pursuant to this Master Agreement. The term Products, supplies and services, and products and services are used interchangeably in these terms and conditions.

Purchasing Entity means a state (as well as the District of Columbia and U.S. territories), city, county, district, other political subdivision of a State, and a nonprofit organization under the laws of some states if authorized by a Participating Addendum, who issues a Purchase Order against the Master Agreement and becomes financially committed to the purchase.

7.3 Term of the Master Agreement

The initial term of this Master Agreement is for two (2) years. This Master Agreement may be extended beyond the original contract period for three (3) additional years at the Lead State's discretion and by mutual agreement and upon review of requirements of Participating Entities, current market conditions, and Contractor performance.

7.4 Amendments

The terms of this Master Agreement shall not be waived, altered, modified, supplemented or amended in any manner whatsoever without prior written approval of the Lead State.

7.5 Assignment/Subcontracts

a. Contractor shall not assign, sell, transfer, subcontract or sublet rights, or delegate responsibilities under this Master Agreement, in whole or in part, without the prior written approval of the Lead State.

b. The Lead State reserves the right to assign any rights or duties, including written assignment of contract administration duties to NASPO Cooperative Purchasing Organization LLC, doing business as NASPO ValuePoint.

7.6 Price and Rate Guarantee Period

All prices and rates must be guaranteed for the first twelve (12) months of the Master Agreement term. Thereafter, requests for additional increases in pricing for contract terms will be limited to once a year. All requests must be made in writing to Lead State Contracting Officer a minimum of 30 days prior to request initiation. Documentation justification regarding any increases must be provided. No price increase will be approved without 30 days written notice and written approval from Lead State Contracting Officer. Any adjustment or amendment to the Master Agreement shall not be effective unless approved by the Lead State. No retroactive adjustments to prices or rates will be allowed.

7.7 Cancellation

Unless otherwise stated, this Master Agreement may be canceled by either party upon 60 days written notice prior to the effective date of the cancellation. Further, any Participating Entity may cancel its participation upon 30 days written notice, unless otherwise limited or stated in the Participating Addendum. Cancellation may be in whole or in part. Any cancellation under this provision shall not affect the rights and obligations attending orders outstanding at the time of cancellation, including any right of and Purchasing Entity to indemnification by the Contractor, rights of payment for Products delivered and accepted, rights attending any warranty or default in performance in association with any Order, and requirements for records administration and audit. Cancellation of the Master Agreement due to Contractor default may be immediate.

7.8 Confidentiality, Non-Disclosure, and Injunctive Relief

7.8.1 Confidentiality. Contractor acknowledges that it and its employees or agents may, in the course of providing a Product under this Master Agreement, be exposed to or acquire information that is confidential to Purchasing Entity's or Purchasing Entity's clients. Any and all information of any form that is marked as confidential or would by its nature be deemed confidential obtained by Contractor or its employees or agents in the performance of this Master Agreement, including, but not necessarily limited to (1) any Purchasing Entity's records, (2) personnel records, and (3) information concerning individuals, is confidential information of Purchasing Entity ("Confidential Information"). Any reports or other documents or items (including software) that result from the use of the Confidential Information by Contractor shall be treated in the same manner as the Confidential Information. Confidential Information does not include information that (1) is or becomes (other than by disclosure by Contractor) publicly known; (2) is furnished by Purchasing Entity to others without restrictions similar to those imposed by this Master Agreement; (3) is rightfully in Contractor's possession without the obligation of nondisclosure prior to the time of its disclosure under this Master Agreement; (4) is obtained

from a source other than Purchasing Entity without the obligation of confidentiality, (5) is disclosed with the written consent of Purchasing Entity or; (6) is independently developed by employees, agents or subcontractors of Contractor who can be shown to have had no access to the Confidential Information.

7.8.2 Non-Disclosure. Contractor shall hold Confidential Information in confidence, using at least the industry standard of confidentiality, and shall not copy, reproduce, sell, assign, license, market, transfer or otherwise dispose of, give, or disclose Confidential Information to third parties or use Confidential Information for any purposes whatsoever other than what is necessary to the performance of Orders placed under this Master Agreement. Contractor shall advise each of its employees and agents of their obligations to keep Confidential Information confidential. Contractor shall use commercially reasonable efforts to assist Purchasing Entity in identifying and preventing any unauthorized use or disclosure of any Confidential Information. Without limiting the generality of the foregoing, Contractor shall advise Purchasing Entity, applicable Participating Entity, and the Lead State immediately if Contractor learns or has reason to believe that any person who has had access to Confidential Information has violated or intends to violate the terms of this Master Agreement, and Contractor shall at its expense cooperate with Purchasing Entity in seeking injunctive or other equitable relief in the name of Purchasing Entity or Contractor against any such person. Except as directed by Purchasing Entity, Contractor will not at any time during or after the term of this Master Agreement disclose, directly or indirectly, any Confidential Information to any person, except in accordance with this Master Agreement, and that upon termination of this Master Agreement or at Purchasing Entity's request, Contractor shall turn over to Purchasing Entity all documents, papers, and other matter in Contractor's possession that embody Confidential Information. Notwithstanding the foregoing, Contractor may keep one copy of such Confidential Information necessary for quality assurance, audits and evidence of the performance of this Master Agreement.

7.8.3 Injunctive Relief. Contractor acknowledges that breach of this section, including disclosure of any Confidential Information, will cause irreparable injury to Purchasing Entity that is inadequately compensable in damages. Accordingly, Purchasing Entity may seek and obtain injunctive relief against the breach or threatened breach of the foregoing undertakings, in addition to any other legal remedies that may be available. Contractor acknowledges and agrees that the covenants contained herein are necessary for the protection of the legitimate business interests of Purchasing Entity and are reasonable in scope and content.

7.8.4 Purchasing Entity Law. These provisions shall be applicable only to extent they are not in conflict with the applicable public disclosure laws of any Purchasing Entity.

7.9 Right to Publish

Throughout the duration of this Master Agreement, Contractor must secure from the Lead State prior approval for the release of any information that pertains to the potential work or activities covered by the Master Agreement. The Contractor shall not make any representations of NASPO Value Point's opinion or position as to the quality or effectiveness of the services that are the subject of this Master

Agreement without prior written consent. Failure to adhere to this requirement may result in termination of the Master Agreement for cause.

7.10 Defaults and Remedies

7.10.1 The occurrence of any of the following events shall be an event of default under this Master Agreement:

(1) Nonperformance of contractual requirements; or

(2) A material breach of any term or condition of this Master Agreement; or

(3) Any certification, representation or warranty by Contractor in response to the solicitation or in this Master Agreement that proves to be untrue or materially misleading; or

(4) Institution of proceedings under any bankruptcy, insolvency, reorganization or similar law, by or against Contractor, or the appointment of a receiver or similar officer for Contractor or any of its property, which is not vacated or fully stayed within thirty (30) calendar days after the institution or occurrence thereof; or

(5) Any default specified in another section of this Master Agreement.

7.10.2 Upon the occurrence of an event of default, Lead State shall issue a written notice of default, identifying the nature of the default, and providing a period of 15 calendar days in which Contractor shall have an opportunity to cure the default. The Lead State shall not be required to provide advance written notice or a cure period and may immediately terminate this Master Agreement in whole or in part if the Lead State, in its sole discretion, determines that it is reasonably necessary to preserve public safety or prevent immediate public crisis. Time allowed for cure shall not diminish or eliminate Contractor's liability for damages, including liquidated damages to the extent provided for under this Master Agreement.

7.10.3 If Contractor is afforded an opportunity to cure and fails to cure the default within the period specified in the written notice of default, Contractor shall be in breach of its obligations under this Master Agreement and Lead State shall have the right to exercise any or all of the following remedies:

7.10.3.1 Exercise any remedy provided by law; and

7.10.3.2 Terminate this Master Agreement and any related Contracts or portions thereof; and

7.10.3.3 Impose liquidated damages as provided in this Master Agreement; and

7.10.3.4 Suspend Contractor from being able to respond to future bid solicitations; and

7.10.3.5 Suspend Contractor's performance; and

7.10.3.6 Withhold payment until the default is remedied.

7.10.4 Unless other specified in the Participating Addendum, in the event of a default under a Participating Addendum, a Participating Entity shall provide a written notice of default as described in this section and have all of the rights and remedies under this paragraph regarding its participation in the Master Agreement, in addition to those set forth in its Participating Addendum. Unless

otherwise specified in a Purchase Order, a Purchasing Entity shall provide written notice of default as described in this section and have all of the rights and remedies under this paragraph and any applicable Participating Addendum with respect to an Order placed by the Purchasing Entity. Nothing in these Master Agreement Terms and Conditions shall be construed to limit the rights and remedies available to a Purchasing Entity under the applicable commercial code.

7.11 Shipping and Delivery

7.11.1.1 The prices are the delivered price to any Purchasing Entity. All deliveries shall be F.O.B. destination, freight pre-paid, with all transportation and handling charges paid by the Contractor. Responsibility and liability for loss or damage shall remain the Contractor's until final inspection and acceptance when responsibility shall pass to the Buyer except as to latent defects, fraud and Contractor's warranty obligations. The minimum shipment amount, if any, will be found in the special terms and conditions. Any order for less than the specified amount is to be shipped with the freight prepaid and added as a separate item on the invoice. Any portion of an order to be shipped without transportation charges that is back ordered shall be shipped without charge.

7.11.1.2 All deliveries will be "Inside Deliveries" as designated by a representative of the Purchasing Entity placing the Order. Inside Delivery refers to a delivery to other than a loading dock, front lobby, or reception area. Specific delivery instructions will be noted on the order form or Purchase Order. Any damage to the building interior, scratched walls, damage to the freight elevator, etc., will be the responsibility of the Offeror. If damage does occur, it is the responsibility of the Offeror to immediately notify the Purchasing Entity placing the Order.

7.11.1.3 All products must be delivered in the manufacturer's standard package. Costs shall include all packing and/or crating charges. Cases shall be of durable construction, good condition, properly labeled and suitable in every respect for storage and handling of contents. Each shipping carton shall be marked with the item description, brand and manufacturer product number, quantity, and the Ordering Entity's Purchase Order number.

7.12 Changes in Contractor Representation

The Contractor must notify the Lead State of changes in the Contractor's key administrative personnel, in writing within 10 calendar days of the change. The Lead State reserves the right to approve changes in key personnel, as identified in the Contractor's proposal. The Contractor agrees to propose replacement key personnel having substantially equal or better education, training, and experience as was possessed by the key person proposed and evaluated in the Contractor's proposal.

7.13 Force Majeure

Neither party to this Master Agreement shall be held responsible for delay or default caused by fire, riot, acts of God and/or war which is beyond that party's reasonable control. The Lead State may terminate this Master Agreement after determining such delay or default will reasonably prevent successful performance of the Master Agreement.

7.14 Indemnification

The Contractor shall defend, indemnify and hold harmless NASPO, NASPO Cooperative Purchasing Organization LLC (doing business as NASPO ValuePoint), the Lead State, Participating Entities, and Purchasing Entities, along with their officers, agents, and employees as well as any person or entity for which they may be liable, from and against third-party claims, damages or causes of action including reasonable attorneys' fees and related costs for any death, injury, or damage to tangible property arising from act(s), error(s), or omission(s) of the Contractor, its employees or subcontractors or volunteers, at any tier, relating to the performance under the Master Agreement.

b. Indemnification – Intellectual Property. The Contractor shall defend, indemnify and hold harmless NASPO, NASPO Cooperative Purchasing Organization LLC (doing business as NASPO ValuePoint), the Lead State, Participating Entities, Purchasing Entities, along with their officers, agents, and employees as well as any person or entity for which they may be liable ("Indemnified Party"), from and against claims, damages or causes of action including reasonable attorneys' fees and related costs arising out of the claim that the Product or its use, infringes Intellectual Property rights ("Intellectual Property Claim") of another person or entity.

(1) The Contractor's obligations under this section shall not extend to any combination of the Product with any other product, system or method, unless the Product, system or method is:

(a) provided by the Contractor or the Contractor's subsidiaries or affiliates;
(b) specified by the Contractor to work with the Product; or
(c) reasonably required, in order to use the Product in its intended manner, and the infringement could not have been avoided by substituting another reasonably available product, system or method capable of performing the same function; or
(d) It would be reasonably expected to use the Product in combination with such product, system or method.

(2) The Indemnified Party shall notify the Contractor within a reasonable time after receiving notice of an Intellectual Property Claim. Even if the Indemnified Party fails to provide reasonable notice, the Contractor shall not be relieved from its obligations unless the Contractor can demonstrate that it was prejudiced in defending the Intellectual Property Claim resulting in increased expenses or loss to the Contractor. If the Contractor promptly and reasonably investigates and defends any Intellectual Property Claim, it shall have control over the defense and settlement of it. However, the Indemnified Party must consent in writing for any money damages or obligations for which it may be responsible. The Indemnified Party shall furnish, at the Contractor's reasonable request and expense, information and assistance necessary for such defense. If the Contractor fails to vigorously pursue the defense or settlement of the Intellectual Property Claim, the Indemnified Party may assume the defense or settlement of it and the Contractor shall be liable for all costs and expenses, including reasonable attorneys' fees and related costs, incurred by the Indemnified Party in the pursuit of the Intellectual Property Claim. Unless otherwise agreed in writing, this section is not subject to any limitations of liability in this Master Agreement or in any other document executed in conjunction with this Master Agreement.

7.15 Independent Contractor

The Contractor shall be an independent contractor. Contractor shall have no authorization, express or implied, to bind the Lead State, Participating States, other Participating Entities,

or Purchasing Entities to any agreements, settlements, liability or understanding whatsoever, and agrees not to hold itself out as agent except as expressly set forth herein or as expressly agreed in any Participating Addendum.

7.16 Individual Customers

Except to the extent modified by a Participating Addendum, each Purchasing Entity shall follow the terms and conditions of the Master Agreement which include the Oklahoma Terms and Conditions and NASPO ValuePoint Master Agreement Terms and Conditions, and applicable Participating Addendum and will have the same rights and responsibilities for their purchases as the Lead State has in the Master Agreement, including but not limited to, any indemnity or right to recover any costs as such right is defined in the Master Agreement and applicable Participating Addendum for their purchases. Each Purchasing Entity will be responsible for its own charges, fees, and liabilities. The Contractor will apply the charges and invoice each Purchasing Entity individually.

7.17 Insurance

a. This section requires insurance in addition to the insurance required by RFP section 4.1.18, Professional and Technical Special Insurance Requirements. Unless otherwise agreed in a Participating Addendum, Contractor shall, during the term of this Master Agreement, maintain in full force and effect, the insurance described in this section. Contractor shall acquire such insurance from an insurance carrier or carriers licensed to conduct business in each Participating Entity's state and having a rating of A-, Class VII or better, in the most recently published edition of A.M. Best's Insurance Reports. Failure to buy and maintain the required insurance may result in this Master Agreement's termination or, at a Participating Entity's option; result in termination of its Participating Addendum.

b. Coverage shall be written on an occurrence basis. The minimum acceptable limits shall be as indicated below:

(1) Commercial General Liability covering premises operations, independent contractors, products and completed operations, blanket contractual liability, personal injury (including death), advertising liability, and property damage, with a limit of not less than $1 million per occurrence/$2 million general aggregate;

(2) Contractor must comply with any applicable State Workers Compensation or Employers Liability Insurance requirements.

c. Contractor shall pay premiums on all insurance policies. Contractor shall provide notice to a Participating Entity who is a state within five (5) business days after Contractor is first aware of expiration, cancellation or nonrenewal of such policy or is first aware that cancellation is threatened or expiration, nonrenewal or expiration otherwise may occur.

d. Prior to commencement of performance, Contractor shall provide to the Lead State a written endorsement to the Contractor's general liability insurance policy or other documentary evidence acceptable to the Lead State that (1) names the Participating States identified in the Request for Proposal as additional insureds, (2) provides for written notice of cancellation shall be delivered in accordance with the policy provisions, and (3) provides that the Contractor's liability

insurance policy shall be primary, with any liability insurance of any Participating State as secondary and noncontributory. Unless otherwise agreed in any Participating Addendum, other state Participating Entities' rights and Contractor's obligations are the same as those specified in the first sentence of this subsection except the endorsement is provided to the applicable state.

e. Contractor shall furnish to the Lead State copies of certificates of all required insurance in a form sufficient to show required coverage within thirty (30) calendar days of the execution of this Master Agreement and prior to performing any work. Copies of renewal certificates of all required insurance shall be furnished within thirty (30) days after any renewal date to the applicable state Participating Entity. Failure to provide evidence of coverage may, at the sole option of the Lead State, or any Participating Entity, result in this Master Agreement's termination or the termination of any Participating Addendum.

f. Coverage and limits shall not limit Contractor's liability and obligations under this Master Agreement, any Participating Addendum, or any Purchase Order.

7.18 Laws and Regulations

Any and all Products offered and furnished shall comply fully with all applicable Federal and State laws and regulations.

7.19 License of Pre-Existing Intellectual Property

Contractor grants to the Purchasing Entity a nonexclusive, perpetual, royalty-free, irrevocable, license to use, publish, translate, reproduce, transfer with any sale of tangible media or Product, perform, display, and dispose of the Intellectual Property, and its derivatives, used or delivered under this Master Agreement, but not created under it ("Pre-existing Intellectual Property"). The Contractor shall be responsible for ensuring that this license is consistent with any third party rights in the Pre-existing Intellectual Property.

7.20 No Waiver of Sovereign Immunity

In no event shall this Master Agreement, any Participating Addendum or any contract or any Purchase Order issued thereunder, or any act of the Lead State, a Participating Entity, or a Purchasing Entity be a waiver of any form of defense or immunity, whether sovereign immunity, governmental immunity, immunity based on the Eleventh Amendment to the Constitution of the United States or otherwise, from any claim or from the jurisdiction of any court.

This section applies to a claim brought against the Participating State only to the extent Congress has appropriately abrogated the Participating State's sovereign immunity and is not consent by the Participating State to be sued in federal court. This section is also not a waiver by the Participating State of any form of immunity, including but not limited to sovereign immunity and immunity based on the Eleventh Amendment to the Constitution of the United States.

7.21 Ordering

a. Master Agreement order and purchase order numbers shall be clearly shown on all acknowledgments, shipping labels, packing slips, invoices, and on all correspondence.

b. The resulting Master Agreements permit Purchasing Entities to define project-specific requirements and informally compete the requirement among companies having a Master Agreement on an "as needed" basis. This procedure may also be used when requirements are

aggregated or other firm commitments may be made to achieve reductions in pricing. This procedure may be modified in Participating Addenda and adapted to the Purchasing Entity's rules and policies. The Purchasing Entity may in its sole discretion determine which Master Agreement Contractors should be solicited for a quote. The Purchasing Entity may select the quote that it considers most advantageous, cost and other factors considered.

c. Each Purchasing Entity will identify and utilize its own appropriate purchasing procedure and documentation. Contractor is expected to become familiar with the Purchasing Entities' rules, policies, and procedures regarding the ordering of supplies and/or services contemplated by this Master Agreement.
d. Contractor shall not begin work without a valid Purchase Order or other appropriate commitment document compliance with the law of the Purchasing Entity.

e. Orders may be placed consistent with the terms of this Master Agreement during the term of the Master Agreement.

f. All Orders pursuant to this Master Agreement, at a minimum, shall include:

(1) The services or supplies being delivered;
(2) The place and requested time of delivery;
(3) A billing address;
(4) The name, phone number, and address of the Purchasing Entity representative;
(5) The price per hour or other pricing elements consistent with this Master Agreement and the contractor's proposal;
(6) A ceiling amount of the order for services being ordered; and
(7) The Master Agreement identifier.

g. All communications concerning administration of Orders placed shall be furnished solely to the authorized purchasing agent within the Purchasing Entity's purchasing office, or to such other individual identified in writing in the Order.

h. Orders must be placed pursuant to this Master Agreement prior to the termination date thereof, but may have a delivery date or performance period up to 120 days past the then-current termination date of this Master Agreement. Contractor is reminded that financial obligations of Purchasing Entities payable after the current applicable fiscal year are contingent upon agency funds for that purpose being appropriated, budgeted, and otherwise made available.

i. Notwithstanding the expiration or termination of this Master Agreement, Contractor agrees to perform in accordance with the terms of any Orders then outstanding at the time of such expiration or termination. Contractor shall not honor any Orders placed after the expiration or termination of this Master Agreement, or otherwise inconsistent with its terms. Orders from any separate indefinite quantity, task orders, or other form of indefinite delivery order arrangement priced against this Master Agreement may not be placed after the expiration or termination of this Master Agreement, notwithstanding the term of any such indefinite delivery order agreement.

7.22 Participants and Scope

a. Contractor may not deliver Products under this Master Agreement until a Participating Addendum acceptable to the Participating Entity and Contractor is executed. The Oklahoma Terms and Conditions and NASPO ValuePoint Master Agreement Terms and Conditions are applicable to any Order by a Participating Entity (and other Purchasing Entities covered by their Participating

Addendum), except to the extent altered, modified, supplemented or amended by a Participating Addendum. By way of illustration and not limitation, this authority may apply to unique delivery and invoicing requirements, confidentiality requirements, defaults on Orders, governing law and venue relating to Orders by a Participating Entity, indemnification, and insurance requirements. Statutory or constitutional requirements relating to availability of funds may require specific language in some Participating Addenda in order to comply with applicable law. The expectation is that these alterations, modifications, supplements, or amendments will be addressed in the Participating Addendum or, with the consent of the Purchasing Entity and Contractor, may be included in the ordering document (e.g. purchase order or contract) used by the Purchasing Entity to place the Order.

b. Use of specific NASPO ValuePoint cooperative Master Agreements by state agencies, political subdivisions and other Participating Entities (including cooperatives) authorized by individual state's statutes to use state contracts are subject to the approval of the respective State Chief Procurement Official. Issues of interpretation and eligibility for participation are solely within the authority of the respective State Chief Procurement Official.

c. Obligations under this Master Agreement are limited to those Participating Entities who have signed a Participating Addendum and Purchasing Entities within the scope of those Participating Addenda. Financial obligations of Participating States are limited to the orders placed by the departments or other state agencies and institutions having available funds. Participating States incur no financial obligations on behalf of other Purchasing Entities. Contractor shall email a fully executed PDF copy of each Participating Addendum to PA@naspovaluepoint.org to support documentation of participation and posting in appropriate data bases.

d. NASPO Cooperative Purchasing Organization LLC, doing business as NASPO ValuePoint, is not a party to the Master Agreement. It is a nonprofit cooperative purchasing organization assisting states in administering the NASPO cooperative purchasing program for state government departments, institutions, agencies and political subdivisions (e.g., colleges, school districts, counties, cities, etc.) for all 50 states, the District of Columbia and the territories of the United States.

e. State Participating Addenda or other Participating Addenda shall not be construed to amend the terms of this Master Agreement between the Lead State and Contractor that prescribe NASPO ValuePoint Program requirements: Term of the Master Agreement; Amendments; Participants and Scope; Administrative Fee; NASPO ValuePoint Summary and Detailed Usage Reports; NASPO ValuePoint Cooperative Program Marketing and Performance Review; NASPO ValuePoint eMarketCenter; Right to Publish; Price and Rate Guarantee Period; and Individual Customers. Any such language shall be void and of no effect.

f. Participating Entities who are not states may under some circumstances sign their own Participating Addendum, subject to the approval of participation by the Chief Procurement Official of the state where the Participating Entity is located. Coordinate requests for such participation through NASPO ValuePoint. Any permission to participate through execution of a Participating Addendum is not a determination that procurement authority exists in the Participating Entity; they must ensure that they have the requisite procurement authority to execute a Participating Addendum.

g. Resale. "Resale" means any payment in exchange for transfer of tangible goods, software, or assignment of the right to services. Subject to any specific conditions included in the solicitation or

Contractor's proposal as accepted by the Lead State, or as explicitly permitted in a Participating Addendum, Purchasing Entities may not resell Products (the definition of which includes services that are deliverables). Absent any such condition or explicit permission, this limitation does not prohibit: payments by employees of a Purchasing Entity for Products; sales of Products to the general public as surplus property; and fees associated with inventory transactions with other governmental or nonprofit entities and consistent with a Purchasing Entity's laws and regulations. Any sale or transfer permitted by this subsection must be consistent with license rights granted for use of intellectual property.

7.23 Payment

Payment for completion of a contract order is normally made within 30 days following the date the entire order is delivered or the date a correct invoice is received, whichever is later. After 45 days the Contractor may assess overdue account charges up to a maximum rate of one percent per month on the outstanding balance. Payments will be remitted by mail. Payments may be made via a State or political subdivision "Purchasing Card" with no additional charge.

7.24 Public Information

This Master Agreement and all related documents are subject to disclosure pursuant to the Purchasing Entity's public information laws.

7.25 Records Administration and Audit

a. The Contractor shall maintain books, records, documents, and other evidence pertaining to this Master Agreement and orders placed by Purchasing Entities under it to the extent and in such detail as shall adequately reflect performance and administration of payments and fees. Contractor shall permit the Lead State, a Participating Entity, a Purchasing Entity, the federal government (including its grant awarding entities and the U.S. Comptroller General), and any other duly authorized agent of a governmental agency, to audit, inspect, examine, copy and/or transcribe Contractor's books, documents, papers and records directly pertinent to this Master Agreement or orders placed by a Purchasing Entity under it for the purpose of making audits, examinations, excerpts, and transcriptions. This right shall survive for a period of seven (7) years following termination of this Agreement or final payment for any order placed by a Purchasing Entity against this Agreement, whichever is later, to assure compliance with the terms hereof or to evaluate performance hereunder. If an audit, litigation, or other action involving the above-referenced documents, required to be maintained for two (2) years from the date that all issues arising out of the action are resolved, or until the end of the seven (7) year retention period, whichever is later.

b. Without limiting any other remedy available to any governmental entity, the Contractor shall reimburse the applicable Lead State, Participating Entity, or Purchasing Entity for any overpayments inconsistent with the terms of the Master Agreement or orders or underpayment of fees found as a result of the examination of the Contractor's records.

c. The rights and obligations herein exist in addition to any quality assurance obligation in the Master Agreement requiring the Contractor to self-audit contract obligations and that permits the Lead State to review compliance with those obligations.

7.26 Administrative Fees

a. The Contractor shall pay to NASPO ValuePoint, or its assignee, a NASPO ValuePoint Administrative Fee of one-quarter of one percent (0.25% or 0.0025) no later than sixty (60) days following the end of each calendar quarter. The NASPO ValuePoint Administrative Fee shall be submitted quarterly and is based on all sales of products and services under the Master Agreement (less any charges for taxes or shipping). The NASPO ValuePoint Administrative Fee is not

negotiable. This fee is to be included as part of the pricing submitted with proposal.

b. Additionally, some states may require an additional fee be paid directly to the state only on purchases made by Purchasing Entities within that state. For all such requests, the fee level, payment method and schedule for such reports and payments will be incorporated into the Participating Addendum that is made a part of the Master Agreement. The Contractor may adjust the Master Agreement pricing accordingly for purchases made by Purchasing Entities within the jurisdiction of the state. All such agreements shall not affect the NASPO ValuePoint Administrative Fee percentage or the prices paid by the Purchasing Entities outside the jurisdiction of the state requesting the additional fee. The NASPO ValuePoint Administrative Fee in subsection 7.26 a. shall be based on the gross amount of all sales (less any charges for taxes or shipping) at the adjusted prices (if any) in Participating Addenda.

7.27 NASPO ValuePoint Summary and Detailed Usage Reports

In addition to other reports that may be required by this solicitation, the Contractor shall provide the following NASPO ValuePoint reports.

a. Summary Sales Data. The Contractor shall submit quarterly sales reports directly to NASPO ValuePoint using the NASPO ValuePoint Quarterly Sales/Administrative Fee Reporting Tool found at http://www.naspo.org/WNCPO/Calculator.aspx. Any/all sales made under this Master Agreement shall be reported as cumulative totals by state. Even if Contractor experiences zero sales during a calendar quarter, a report is still required. Reports shall be due no later than thirty (30) days following the end of the calendar quarter (as specified in the reporting tool).

b. Detailed Sales Data. Contractor shall also report detailed sales data by: (1) state; (2) entity/customer type, e.g. local government, higher education, K12, non-profit; (3) Purchasing Entity name; (4) Purchasing Entity bill-to and ship-to locations; (4) Purchasing Entity and Contractor Purchase Order identifier/number(s); (5) Purchase Order Type (e.g. sales order, credit, return, upgrade, determined by industry practices); (6) Purchase Order date; (7) Ship Date; (8) and line item description, including product number if used. The report shall be submitted in any form required by the solicitation. Reports are due on a quarterly basis and must be received by the Lead State and NASPO ValuePoint Cooperative Development Team no later than thirty (30) days after the end of the reporting period. Reports shall be delivered to the Lead State and to the NASPO ValuePoint Cooperative Development Team electronically through a designated portal, email, CD-ROM, flash drive or other method as determined by the Lead State and NASPO ValuePoint. Detailed sales data reports shall include sales information for all sales under Participating Addenda executed under this Master Agreement. The format for the detailed sales data report is in shown in Attachment I – Usage Reporting Template

c. Reportable sales for the summary sales data report and detailed sales data report includes sales to employees for personal use where authorized by the solicitation and the Participating Addendum. Report data for employees should be limited to ONLY the state and entity they are participating under the authority of (state and agency, city, county, school district, etc.) and the amount of sales. No personal identification numbers, e.g. names, addresses, **social security numbers or any other numerical identifier**, may be submitted with any report.

d. Contractor shall provide the NASPO ValuePoint Cooperative Development Coordinator with an executive summary each quarter that includes, at a minimum, a list of states with an active Participating Addendum, states that Contractor is in negotiations with and any Participating Addendum roll out or implementation activities and issues. NASPO ValuePoint Cooperative

Development Coordinator and Contractor will determine the format and content of the executive summary. The executive summary is due thirty (30) days after the conclusion of each calendar quarter.

e. Timely submission of these reports is a material requirement of the Master Agreement. The recipient of the reports shall have exclusive ownership of the media containing the reports. The Lead State and NASPO ValuePoint shall have a perpetual, irrevocable, non-exclusive, royalty free, transferable right to display, modify, copy, and otherwise use reports, data and information provided under this section.

7.28 Inspection and Acceptance

a. Where the Master Agreement or an Order does not otherwise specify a process for inspection and Acceptance, this section governs. This section is not intended to limit rights and remedies under the applicable commercial code.

b. All Products are subject to inspection at reasonable times and places before Acceptance. Contractor shall provide right of access to the Lead State, or to any other authorized agent or official of the Lead State or other Participating or Purchasing Entity, at reasonable times, in order to monitor and evaluate performance, compliance, and/or quality assurance requirements under this Master Agreement. Products that do not meet specifications may be rejected. Failure to reject upon receipt, however, does not relieve the contractor of liability for material (nonconformity that substantial impairs value) latent or hidden defects subsequently revealed when goods are put to use. Acceptance of such goods may be revoked in accordance with the provisions of the applicable commercial code, and the Contractor is liable for any resulting expense incurred by the Purchasing Entity related to the preparation and shipping of Product rejected and returned, or for which Acceptance is revoked.

c. If any services do not conform to contract requirements, the Purchasing Entity may require the Contractor to perform the services again in conformity with contract requirements, at no increase in Order amount. When defects cannot be corrected by re-performance, the Purchasing Entity may require the Contractor to take necessary action to ensure that future performance conforms to contract requirements; and reduce the contract price to reflect the reduced value of services performed.

d. The warranty period shall begin upon Acceptance.

7.29 Warranty

Unless a warranty is otherwise proposed by Contractor and accepted by the Lead State in accordance with RFP section 4.1.8, this section governs. The Contractor warrants for a period of one year from the date of Acceptance that: (a) the Product performs according to all specific claims that the Contractor made in its response to the solicitation, and (b) (b) the Product is free of defects in materials and workmanship. Upon breach of the warranty, the Contractor will repair or replace (at no charge to the Purchasing Entity) the Product whose nonconformance is discovered and made known to the Contractor. If the repaired and/or replaced Product proves to be inadequate, or fails of its essential purpose, the Contractor will refund the full amount of any payments that have been made. The rights and remedies of the parties under this warranty are in addition to any other rights and remedies of the parties provided by law or equity, including, without limitation, actual damages, and, as applicable and awarded under the law, to a prevailing party, reasonable attorneys' fees and costs.

7.30 NASPO ValuePoint Cooperative Program Marketing and Performance Review

a. Contractor agrees to work cooperatively with NASPO ValuePoint personnel. Contractor agrees to present plans to NASPO ValuePoint for the education of Contractor's contract administrator(s) and sales/marketing workforce regarding the Master Agreement contract, including the competitive nature of NASPO ValuePoint procurements, the Master agreement and participating addendum process, and the manner in which qualifying entities can participate in the Master Agreement.

b. Contractor agrees to participate in an annual contract performance review at a location selected by the Lead State and NASPO ValuePoint, which may include a discussion of marketing action plans, target strategies, marketing materials, as well as Contractor reporting and timeliness of payment of administration fees.

7.31 Title of Product

Upon Acceptance by the Purchasing Entity, Contractor shall convey to Purchasing Entity title to the Product free and clear of all liens, encumbrances, or other security interests. Transfer of title to the Product shall include an irrevocable and perpetual license to use any Embedded Software in the Product. If Purchasing Entity subsequently transfers title of the Product to another entity, Purchasing Entity shall have the right to transfer the license to use the Embedded Software with the transfer of Product title. A subsequent transfer of this software license shall be at no additional cost or charge to either Purchasing Entity or Purchasing Entity's transferee.

7.32 Waiver of Breach

Failure of the Lead State, Participating Entity, or Purchasing Entity to declare a default or enforce any rights and remedies shall not operate as a waiver under this Master Agreement or Participating Addendum. Any waiver by the Lead State, Participating Entity, or Purchasing Entity must be in writing. Waiver by the Lead State or Participating Entity of any default, right or remedy under this Master Agreement or Participating Addendum, or by Purchasing Entity with respect to any Purchase Order, or breach of any terms or requirements of this Master Agreement, a Participating Addendum, or Purchase Order shall not be construed or operate as a waiver of any subsequent default or breach of such term or requirement, or of any other term or requirement under this Master Agreement, Participating Addendum, or Purchase Order.

7.33 Assignment of Antitrust Rights

Contractor irrevocably assigns to a Participating Entity who is a State any claim for relief or cause of action which the Contractor now has or which may accrue to the Contractor in the future by reason of any violation of state or federal antitrust laws (15 U.S.C. § 1-15 or a Participating Entity's state antitrust provisions), as now in effect and as may be amended from time to time, in connection with any goods or services provided to the Contractor for the purpose of carrying out the Contractor's obligations under this Master Agreement or Participating Addendum, including, at a Participating Entity's option, the right to control any such litigation on such claim for relief or cause of action.

7.34 Debarment

The Contractor certifies that neither it nor its principals are presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction (contract) by any governmental department or agency. This certification represents a recurring certification made at the time any Order is placed under this Master Agreement. If the Contractor cannot certify this statement, attach a written explanation for review by the Lead State.

7.35 Governing Law and Venue

a. The procurement, evaluation, and award of the Master Agreement shall be governed by and

construed in accordance with the laws of the Lead State sponsoring and administering the procurement. The construction and effect of the Master Agreement after award shall be governed by the law of the state serving as Lead State (in most cases also the Lead State). The construction and effect of any Participating Addendum or Order against the Master Agreement shall be governed by and construed in accordance with the laws of the Participating Entity's or Purchasing Entity's State.

b. Unless otherwise specified in the RFP, the venue for any protest, claim, dispute or action relating to the procurement, evaluation, and award is in the Lead State. Venue for any claim, dispute or action concerning the terms of the Master Agreement shall be in the state serving as Lead State. Venue for any claim, dispute, or action concerning any Order placed against the Master Agreement or the effect of a Participating Addendum shall be in the Purchasing Entity's State.

c. If a claim is brought in a federal forum, then it must be brought and adjudicated solely and exclusively within the United States District Court for (in decreasing order of priority): the Lead State for claims relating to the procurement, evaluation, award, or contract performance or administration if the Lead State is a party; the Participating State if a named party; the Participating Entity state if a named party; or the Purchasing Entity state if a named party.

7.36 NASPO ValuePoint eMarket Center

a. In July 2011, NASPO ValuePoint entered into a multi-year agreement with SciQuest, Inc. whereby SciQuest will provide certain electronic catalog hosting and management services to enable eligible NASPO ValuePoint's customers to access a central online website to view and/or shop the goods and services available from existing NASPO ValuePoint Cooperative Contracts. The central online website is referred to as the NASPO ValuePoint eMarket Center.

b. The Contractor will have visibility in the eMarket Center through Ordering Instructions. These Ordering Instructions are available at no cost to the Contractor and provide customers information regarding the Contractors website and ordering information. The Contractor is required at a minimum to participate in the eMarket Center through Ordering Instructions.

c. At a minimum, the Contractor agrees to the following timeline: NASPO ValuePoint eMarket Center Site Admin shall provide a written request to the Contractor to begin Ordering Instruction process. The Contractor shall have thirty (30) days from receipt of written request to work with NASPO ValuePoint to provide any unique information and ordering instructions that the Contractor would like the customer to have.

d. If the solicitation requires either a catalog hosted on or integration of a punchout site with eMarket Center or either solution is proposed by a Contractor and accepted by the Lead State, the provisions of the eMarket Center Appendix to these NASPO ValuePoint Master Agreement Terms and Conditions apply.

eMarket Center Appendix

a. This Appendix applies whenever a catalog hosted by or integration of a punchout site with eMarket Center is required by the solicitation or either solution is proposed by a Contractor and accepted by the Lead State.

b. Supplier's Interface with the eMarket Center. There is no cost charged by SciQuest to the Contractor for loading a hosted catalog or integrating a punchout site.

c. At a minimum, the Contractor agrees to the following:

(1) Implementation Timeline: NASPO ValuePoint eMarket Center Site Admin shall provide a written request to the Contractor to begin enablement process. The Contractor shall have fifteen (15) days from receipt of written request to work with NASPO ValuePoint and SciQuest to set up an enablement schedule, at which time SciQuest's technical documentation shall be provided to the Contractor. The schedule will include future calls and milestone dates related to test and go live dates. The contractor shall have a total of Ninety (90) days to deliver either a (1) hosted catalog or (2) punch-out catalog, from date of receipt of written request.

(2) NASPO ValuePoint and SciQuest will work with the Contractor, to decide which of the catalog structures (either hosted or punch-out as further described below) shall be provided by the Contractor. Whether hosted or punch-out, the catalog must be strictly limited to the Contractor's awarded contract offering (e.g. products and/or services not authorized through the resulting cooperative contract should not be viewable by NASPO ValuePoint Participating Entity users).

(a) Hosted Catalog. By providing a hosted catalog, the Contractor is providing a list of its awarded products/services and pricing in an electronic data file in a format acceptable to SciQuest, such as Tab Delimited Text files. In this scenario, the Contractor must submit updated electronic data [Insert Time Frame Here] to the eMarket Center for the Lead State's approval to maintain the most up-to-date version of its product/service offering under the cooperative contract in the eMarket Center.

(b) Punch-Out Catalog. By providing a punch-out catalog, the Contractor is providing its own online catalog, which must be capable of being integrated with the eMarket Center as a. Standard punch-in via Commerce eXtensible Markup Language (cXML). In this scenario, the Contractor shall validate that its online catalog is up-to-date by providing a written update [every Insert Time Frame Here] to the Lead State stating they have audited the offered products/services and pricing listed on its online catalog. The site must also return detailed UNSPSC codes (as outlined in line 3) for each line item. Contractor also agrees to provide e-Quote functionality to facilitate volume discounts.

d. Revising Pricing and Product Offerings: Any revisions to product/service offerings (new products, altered SKUs, new pricing etc.) must be pre-approved by the Lead State and shall be subject to any other applicable restrictions with respect to the frequency or amount of such revisions. However, no cooperative contract enabled in the eMarket Center may include price changes on a more frequent basis than once per quarter. The following conditions apply with respect to hosted catalogs:

(1). Updated pricing files are required by the 1st of the month and shall go into effect in the eMarket Center on the [1st day of the following month (i.e. file received on 1/01/13 would be effective in the eMarket Center on 2/01/13)]. Files received after the 1st of the

month may be delayed up to a month (i.e. file received on 11/06/09 would be effect in the eMarket Center on 1/01/10).

(2) Lead State-approved price changes are not effective until implemented within the eMarket Center. Errors in the Contractor's submitted pricing files will delay the implementation of the price changes in eMarket Center.

e. Supplier Network Requirements: Contractor shall join the SciQuest Supplier Network (SQSN) and shall use the SciQuest's Supplier Portal to import the Contractor's catalog and pricing, into the SciQuest system, and view reports on catalog spend and product/pricing freshness. The Contractor can receive orders through electronic delivery (cXML) or through low-tech options such as fax. More information about the SQSN can be found at: www.sciquest.com or call the SciQuest Supplier Network Services team at 800-233-1121.

f. Minimum Requirements: Whether the Contractor is providing a hosted catalog or a punch-out catalog, the Contractor agrees to meet the following requirements:

(1) Catalog must contain the most current pricing, including all applicable administrative fees and/or discounts, as well as the most up-to-date product/service offering the Contractor is authorized to provide in accordance with the cooperative contract; and

(2) The accuracy of the catalog must be maintained by Contractor throughout the duration of the cooperative contract between the Contractor and the Contract Administrator; and

(3) The Catalog must include a Lead State contract identification number; and

(4) The Catalog must include detailed product line item descriptions; and

(5) The Catalog must include pictures when possible; and

(6) The Catalog must include any additional NASPO ValuePoint and Participating Addendum requirements. Although suppliers in the SQSN normally submit one (1) catalog, it is possible to have multiple contracts applicable to different NASPO ValuePoint Participating Entities. For example, a supplier may have different pricing for state government agencies and Board of Regents institutions. Suppliers have the ability and responsibility to submit separate contract pricing for the same catalog if applicable. The system will deliver the appropriate contract pricing to the user viewing the catalog.

g. Order Acceptance Requirements: Contractor must be able to accept Purchase Orders via fax or cXML. The Contractor shall provide positive confirmation via phone or email within 24 hours of the Contractor's receipt of the Purchase Order. If the Purchasing Order is received after 3pm EST on the day before a weekend or holiday, the Contractor must provide positive confirmation via phone or email on the next business day.

h. UNSPSC Requirements: Contractor shall support use of the United Nations Standard Product and Services Code (UNSPSC). UNSPSC versions that must be adhered to are driven by SciQuest for the suppliers and are upgraded every year. NASPO ValuePoint reserves the right to migrate to future versions of the UNSPSC and the Contractor shall be required to support the migration effort. All line items, goods or services provided under the resulting statewide contract must be associated to a UNSPSC code. All line items must be identified at the most detailed UNSPSC level indicated

by segment, family, class and commodity. More information about the UNSPSC is available at: http://www.unspsc.com and http://www.unspsc.com/FAQs.asp#howdoesunspscwork.

i. Applicability: Contractor agrees that NASPO ValuePoint controls which contracts appear in the eMarket Center and that NASPO ValuePoint may elect at any time to remove any supplier's offering from the eMarket Center.

j. The Lead State reserves the right to approve the pricing on the eMarket Center. This catalog review right is solely for the benefit of the Lead State and Participating Entities, and the review and approval shall not waive the requirement that products and services be offered at prices (and approved fees) required by the Master Agreement.

k. Several NASPO ValuePoint Participating Entities currently maintain separate SciQuest eMarketplaces, these Participating Entities do enable certain NASPO ValuePoint Cooperative Contracts. In the event one of these entities elects to use this NASPO ValuePoint Cooperative Contract (available through the eMarket Center) but publish to their own eMarketplace, the Contractor agrees to work in good faith with the entity and NASPO ValuePoint to implement the catalog. NASPO ValuePoint does not anticipate that this will require substantial additional efforts by the Contractor; however, the supplier agrees to take commercially reasonable efforts to enable such separate SciQuest catalogs.

7.37 Contract Provisions for Orders Utilizing Federal Funds

Pursuant to Appendix II to 2 Code of Federal Regulations (CFR) Part 200, Contract Provisions for Non-Federal Entity Contracts Under Federal Awards, Orders funded with federal funds may have additional contractual requirements or certifications that must be satisfied at the time the Order is placed or upon delivery. These federal requirements may be proposed by Participating Entities in Participating Addenda and Purchasing Entities for incorporation in Orders placed under this master agreement.

8 ATTACHMENT B: SCOPE OF WORK

8.1 Introduction

The State of Oklahoma, Office of Management and Enterprise Services (OMES), Central Purchasing, in furtherance of the NASPO ValuePoint Cooperative Purchasing Program, is releasing this Request for Proposal (RFP) to establish Master Agreement Contracts with qualified manufacturers' for **Public Safety/Law Enforcement Video and Vehicle Mounted Equipment.**

The goal of this RFP is to provide State(s) requirements for competitive proposals along with value-added solutions which allow State and Local Governments to easily equip their public safety transportation equipment and employees with the best competitive pricing, cutting edge technology, and superior customer services without the need for individual competitive proposals.

As permitted by Attachment A, the NASPO ValuePoint Master Agreement Terms and Conditions, authorized governmental entities in any State are welcome to use the resulting Master Agreements through NASPO Valuepoint with the approval of the State Chief Procurement Official. Upon final award of the Master Agreements, Awarded Suppliers are able to sign Participating Addendums (PA) at the option of the Participating States. These States reserve the right to add their individual State specific terms and conditions, as well as their own contract management or administrative fee.

For the purpose of this RFP, there are 4 product bands identified below which may be awarded. Respondents must only respond to the Bands in which they manufacture or are authorized to distribute the defined products. The State of Oklahoma intends to establish multiple awards throughout the bands, and reserves the right to eliminate any band not meeting full expectations from the final award.

8.2 Product Bands

BAND 1: Body Worn Video Cameras and Recording Devices

BAND 2: Vehicle Mounted Video and Recording Devices

BAND 3: Video Storage, Data Security, Software, and Peripherals

BAND 4: Vehicle Mounted Equipment

8.3 Product Band Definitions and Minimum Requirements

This RFP is divided into four (4) individual product bands. Each band shall include all associated hardware, software, mounting equipment and services. With the volatile speed of technology designs, growing demands and unique customizable configurations, these bands shall remain flexible and may be redefined during the life of this contract.

It is the intent upon award to have an offering of Good, Better, and Best to allow for utilization for both small and large public safety organizations.

Note: the following items will not be included in this contract award: Body Armor, LED Light Bars, Public Safety Radios, Radar, and Lidar Equipment. These items are on separate NASPO ValuePoint Master Agreements.

8.4 BAND 1: BODY WORN VIDEO CAMERAS AND RECORDING DEVICES.

To include, but not limited to: Mobile Camera and Recording Equipment which is not permanently installed on a fixed surface. This may be attached to a person, mounted on the chest, belt, hat, or glasses etc. Equipment shall be able to capture video from the Officer's perspective and store the recorded video on a secure hosted website, or secure local storage solution.

8.4.1 Minimum Requirements:

SPEC REQUIREMENT	GOOD	BETTER	BEST
Resolution	640 x 480	1280 x 960	1920 x 1080
Format	AVI	MPEG4	
Field of View	Min. 65 degrees	Min. 90 degrees	Min. 120 degrees
LUX	1.5	1	0.5
Record Life	2.5	4	8
Standby Life	6	12	72
Pre Record Mandatory Y/N	N	Y	Y
Storage	16 GB	32 GB	64 GB
Battery Charge Time	Max 8 hours	Max 6 hours	Max 6 hours
Record Time	4 hours or less	5-7 hours	8 and more hours
Frame Rate	25 FPS	30 FPS	30 FPS
Recharging Options	USB Cable	USB Cable or Docking Station	USB Cable or Docking Station
Recording Indicator	Visual Only	Visual & Sound Option	Visual & Sound Option
Weatherproof/Construction	IP65	IP66	IP67 or IP68
Displays remaining Storage Level	Graph	Hours/Minutes	Hours/Minutes & Audible/Visual Warning
Rotatable Lens	No	Yes	Yes
Covert mode triggerable	Yes/Predefined	Yes/User Triggerable	Yes/User triggerable
Video Compression	Lossy	Lossless	Lossless
Sound Quality	Standard	Hi-Fi	HD Sound

8.4.2 Technical Mandatory Requirements

8.4.2.1 All wiring, cables, clips, or other methods of attachment required for the device to function properly shall be designed to disengage to prevent the wearer from becoming entangled. Describe what type of external cabling your device uses and any features which may allow the device to continue operating or to tag an interruption.

8.4.2.2 The System shall produce a method to log all recordings, deletions, and edits. These reports shall also indicate which items have been deleted, edited, the time and date when changes were made, and who performed the actions. Describe the type of capabilities of proposed system logs and reports, method of generating documents, estimated time of completing reports, and typical training time frame to master system reports.

8.4.2.3 The system shall prevent unauthorized alteration or deletion of records and recorded data.

8.4.2.4 . The system shall be capable to establish the start of a predetermined retention period for any data stored by a date or other event trigger. Describe your capabilities to set automated retention schedules.

8.4.2.5 Describe in detail how your system can resume original retention schedules after recorded data has been used for an investigation, litigation, or any other legal action and said activity has been concluded.

8.4.2.6 The system shall have total capability to access, search, and retrieve recorded data entirely throughout the predetermined retention period. Describe systems indexing and search processes.

8.4.2.7 The capability to restrict access to certain videos is required. Describe how your system can secure recorded data from unauthorized access, regardless of classification, and apply key users viewing privileges.

8.5 BAND 2: VEHICLE MOUNTED VIDEO AND RECORDING DEVICES

Includes permanently mounted video equipment. Intended use is for police vehicles, public transit, school buses, and other public safety vehicles. Additional, products can be proposed and available for use by a variety of law enforcement applications, which may also include state police, marine police, corrections, game and inland fisheries, forestry, border surveillance, educational campuses, as well as local fire departments and other emergency first responder needs.

8.5.1 Minimum Requirements:

All mobile video systems and related audio equipment must conform to the applicable minimum standards as set by the following:

a) Electronic Industries Association (EIA)

b) Federal Communications Commission rules and regulations (FCC)

c) Institute of Electrical and Electronic Engineers (IEEE)

d) International Electro technical Commission (IEC)

e) International Organization for Standardization (ISO)

f) National Fire Protection International (NFPA)

g) National Highway Traffic Safety Administration (NHTSA)

h) Society of Automotive Engineers (SAE)

i) Underwriters Laboratories Inc. (UL)

j) Underwriters Laboratories of Canada (ULC)

Any items installed in the interior of the vehicle shall meet the requirements stated in Federal Motor Vehicle Safety Standards.

Manufacturers shall provide the customer the necessary brackets, mounting hardware, and installation instructions that if followed properly will ensure the vendor's equipment is installed in accordance with all appropriate Federal Motor Vehicle Safety Standards (FMVSS) that are in place at the time of the contract between the vendor and the State(s).

8.5.2 Technical Mandatory Minimum Requirements

Screen/Monitor	Minimum 3 inches diagonal with color display
Temp Range	Sub Zero to 120 Degrees Fahrenheit
Viewing Angle/Diag.	Rotation of 360 Degrees or 180 front facing
Front Field of View	Minimum 24 feet Width, 35 feet full wide angle
Signal to noise Radio	Of at least 46 db.
Microphone	Wireless audio from range of 1000 feet
Activation	Record Button, Emergency Lights and/or Siren
Duration	Record Events uninterrupted for minimum of
	3.5 hours.
Power Source	Between 9 and 18 volts.
Record Indicators	Illuminated indicator visible outside and front seat
Camera Lens	Autofocus/Auto exposure; auto white balance
Erasure Prevention	Erasing, Altering, and/or Recording over data
Time Stamp	Video, Audio, Metadata shall be consistent
Audit Log	Name/ID, automated verification-min 128 bit hash value
Equipment Diagnostic	Shall perform self-test to complete functionality.
	Storage Space Remaining
	Shall send notification to user for any malfunction
Aspect Ratio:	16:9
High Definition Resolution	720p
Internal Storage	128 GB

8.5.3 Mandatory Technical Requirements

8.5.3.1 Product must not interfere with normal operation of the emergency vehicle; and must not create a safety risk for operator or passengers. Shall not cause interference with any other electronic systems in operation (radio, computer, speed detection, etc.)

8.5.3.2 Product shall have “low battery’ indicators and provide process for system to power down without causing any damage to recording device or data storage unit.

8.5.3.3 Product must be a complete mountable solution to accommodate different types of vehicles, (i.e. Ford Explorers, Dodge Chargers, Chevy Impalas and Tahoes, Public Transportation Bus or Subway cars) without degrading original equipment performance.

8.5.3.4 Monitor should include a non-glare touch screen or mechanism to control video in the vehicle.

8.5.3.5 System recording should be in a non-proprietary video format.

8.5.3.6 Recording should be both audio and video, with separate channels and capabilities of recording events inside and outside the vehicle simultaneously.

8.5.3.7 System must have wireless upload capabilities, and if upload process is interrupted, upload will resume from point of interruption.

8.5.3.8 System shall have a secure method to access camera system to prevent any unauthorized access to recording device.

8.5.3.9 System shall have ability to allow user input for data/metadata associated with tagged video.

8.5.3.10 Digital video file must provide ability to determine and authenticate an original file or indicate if file has been modified

8.6 BAND 3: Video Storage, Data Security, Software, and Peripherals

This band will include all supporting equipment and/or services for video storage, including Government cloud services or local secured storage systems. Data management tools, software with related maintenance and/or license fees, related peripherals. Band 3 is not considered to be a hardware category without the purchase of bundled video products and/or accessories.

8.6.1 Mandatory Requirements for Data Management and Storage Services:

8.6.1.1 . Offeror must contractually commit in writing to managing data in accordance with the FBI’s Criminal Justice Information Services (CJIS) Security Policy by signing the Appendix H – Security Addendum (Attachment F) with each requesting Agency.

8.6.1.2 . Offeror must provide document that the personnel working in your cloud provider’s data center passed a fingerprint-based CJIS background check provided by the FBI or your state’s CJIS office

8.6.1.3 Offeror must contractually commit to audits to demonstrate continued adherence and detail providing full support for CJIS compliance?

8.6.1.4 Please reference Criminal Justice Information Services (CJIS) Security Policy, Version 5.4, dated 10/06/2015, https://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center

or most current security policy as issued.

8.6.1.5 Offeror must be able to provide a separate, fully isolated cloud platform for U.S. federal, state, and local government customers.

8.6.1.6 . Offeror must agree and certify that the individual State(s) will retain ownership of all data.

8.6.1.7 Offeror must attest that all State and Local Government data will be kept within the continental limits of the United States.

8.6.1.8 Offeror must explain chain of custody process, all associated user fees, access fees, switch/change fees, and methods of data retrieval.

8.6.1.9 All work done by the contractor must be done in the continental United States.

8.6.1.10 Proposed solution must have the ability to share video evidence with groups inside and outside of Agency, with no proprietary file formats to view video.

8.6.1.11 Agency may require controlled access to evidence; define roles, and permissions, users, and passwords.

8.6.1.12 Must be capable of creating multiple evidence files, tags, markers, indexes, and clips without altering original video

8.6.1.13 Video management system should contain built-in redaction system for both audio and video.

8.7 BAND 4: VEHICLE MOUNTED EQUIPMENT.

Band 4 will include items such as, but not limited to: Consoles, Partitions, Window Armor, Vehicle Armor, Pushbumpers, Prisoner Seats, K9 Enclosures and Accessories, Gun Locks, Trunk Trays, Cargo Slides, Printer Mounts, Computer Mounts, Docking Stations, Anti-Theft Devices, Spotlights, Idle Systems, Air Bag Cutouts, Skid Plates, Trunk Organizers, Cargo Barriers, Wiring Harness, Gun Racks, Siren Speakers, etc.

Band 4 encompasses a wide grouping of varied equipment. To ensure participating end users have needs covered; please provide category discounts along with brand name to products you are proposing.

Reference Pricing Section 5 for cost submittal instructions, and Attachment D – Band 4

9 ATTACHMENT C – OKLAHOMA TERMS AND CONDITIONS FOR AWARD

State of Oklahoma
Office of Management and Enterprise Services

STATE OF OKLAHOMA
TERMS AND CONDITIONS

9.1 Definitions

Acquisition
The term ("Acquisition") means items, products, materials, supplies, services, and equipment a state agency acquires by purchase, lease purchase, lease with option to purchase, or rental pursuant to the Oklahoma Central Purchasing Act.

Addendum or Addenda
The term ("Addendum or Addenda") means a document used to effect a contract change or modification in or more provisions of an existing a contract.

Lead State
The term ("Lead State") means the State centrally administering any resulting Master Agreement. The State of Oklahoma is the Lead State for this Master Agreement.

9.2 Master Agreement Modification

The terms of this Master Agreement shall not be waived, altered, modified, supplemented or amended in any manner whatsoever without prior written approval of the State Purchasing Director of the Lead State.

9.3 Indemnification

In connection with indemnification under the Master Agreement, when the Lead State or any Lead state agency is a named defendant in any filed or threatened lawsuit, the defense of the Lead State or Lead State agency shall be coordinated by the Attorney General of Oklahoma or, in the alternative, the Attorney General of Oklahoma may authorize the Vendor to control the defense and any related settlement negotiations; provided, however, Contractor shall not agree to any settlement of claims against the Lead State or Lead State agency without obtaining advance written concurrence from the State Attorney General. If the Attorney General of Oklahoma does not authorize sole control of the defense and settlement negotiations to Contractor, Contractor shall have authorization to equally

participate in any proceeding related to the indemnity obligation under the Master Agreement and shall remain responsible to indemnify the applicable Indemnified Parties.

9.4 Audits and Records Clause

For transactions between the Lead State and the Contractor, the Contractor shall maintain books, records, documents, and other evidence pertaining to this Master Agreement and orders placed by Purchasing Entities under it to the extent and in such detail as shall adequately reflect performance and administration of payments and fees. Contractor shall permit the Lead State, a Participating Entity, a Purchasing Entity, the federal government (including its grant awarding entities and the U.S. Comptroller General), and any other duly authorized agent of a governmental agency, to audit, inspect, examine, copy and/or transcribe Contractor's books, documents, papers and records directly pertinent to this Master Agreement or orders placed by a Purchasing Entity under it for the purpose of making audits, examinations, excerpts, and transcriptions. This right shall survive for a period of seven (7) years following termination of this Agreement or final payment for any order placed by a Purchasing Entity against this Agreement, whichever is later, to assure compliance with the terms hereof or to evaluate performance hereunder. If an audit, litigation, or other action involving the above-referenced documents, required to be maintained for two (2) years from the date that all issues arising out of the action are resolved, or until the end of the seven (7) year retention period, whichever is later.

Without limiting any other remedy available to any governmental entity, the Contractor shall reimburse the applicable Lead State, Participating Entity, or Purchasing Entity for any overpayments inconsistent with the terms of the Master Agreement or orders or underpayment of fees found as a result of the examination of the Contractor’s records.

The rights and obligations herein exist in addition to any quality assurance obligation in the Master Agreement requiring the Contractor to self-audit contract obligations and that permits the Lead State to review compliance with those obligations.

9.5 Assignment/Subcontracts

Contractor shall not assign, sell, transfer, subcontract or sublet rights, or delegate responsibilities under this Master Agreement, in whole or in part, without the prior written approval of the State Purchasing Director of the Lead State.

9.6 Payment

For transactions between the Lead State and the Contractor, invoices are to be paid in arrears after products have been delivered and accepted or services provided and accepted pursuant to 74 O.S. § 85.44(B). Payment by the Lead State will be made within no more than forty-five (45) days from the date a proper invoice is received and the goods have been delivered and accepted or services provided and accepted pursuant to 62 O.S. § 34.71. Interest on late payments made by the Lead State is governed by 62 O.S. § 34.72.

9.7 Changes in Contractor Representation

The Contractor must notify the State Purchasing Director of the Lead State of changes in the Contractor's key administrative personnel, in writing within 10 calendar days of the change. The State Purchasing Director of the Lead State reserves the right to approve changes in key personnel, as identified in the Contractor's proposal. The Contractor agrees to propose replacement key personnel having substantially equal or better education, training, and experience as was possessed by the key person proposed and evaluated in the Contractor's proposal.

9.5. Right to Publish

Throughout the duration of this Master Agreement, Contractor must secure from the State Purchasing Director of the Lead State prior approval for the release of any information that pertains to the potential work or activities covered by the Master Agreement. The Contractor shall not make any representations of NASPO Value Point's opinion or position as to the quality or effectiveness of the services that are the subject of this Master Agreement without prior written consent. Failure to adhere to this requirement may result in termination of the Master Agreement for cause.

9.8 Certification Regarding Debarment, Suspension, and Other Responsibility Matters

The Contractor certifies that the Contractor and it principals:

A. Are not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded by any federal, state or local department or agency;

B. Have not within a three-year period preceding the Contract been convicted of or had a civil judgment rendered against them for commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (federal, state or local) contract; for violation of federal or state antitrust statutes; commission of embezzlement, theft, forgery, bribery, falsification or destruction of records; making false statements or receiving stolen property;

C. Are not presently indicted for or otherwise criminally or civilly charged by a governmental entity (federal, state or local) with commission of any of the foregoing offenses enumerated in this certification; and

D. Have not within a three-year period preceding this Contract had one or more public (federal, state or local) contracts terminated for cause or default.

If the Contractor cannot certify this statement, attach a written explanation for review by the Lead State.

9.9 Choice of Venue

Unless otherwise specified in the RFP, the venue for any protest, claim, dispute or action relating to the procurement, evaluation, and award is in Oklahoma County, Oklahoma. Venue for any claim, dispute or action concerning the terms of the Master Agreement shall be in Oklahoma County, Oklahoma. Venue for any claim, dispute, or action concerning any Order placed against the Master Agreement or the effect of a Participating Addendum shall be in the Purchasing Entity's State.

If a claim is brought in a federal forum, then it must be brought and adjudicated solely and exclusively within the United States District Court for (in decreasing order of priority): the Lead State for claims relating to the procurement, evaluation, award, or contract performance or administration if the Lead State is a party; the Participating State if a named party; the Participating Entity state if a named party; or the Purchasing Entity state if a named party. Where the claim is adjudicated in the United States District Court of the Lead State, it must be brought and adjudicated in the Western District.

9.10 Extension of the Master Agreement

The Lead State may extend the term of this Master Agreement for up to ninety (90) day intervals if mutually agreed upon by the State Purchasing Director of the Lead State and the Contractor.

9.11 Gratuities

The right of the Contractor to perform under this Master Agreement may be terminated by written notice if the Procurement Official as specified in E.4. of the Solicitation determines that the Contractor, or its agent or another representative offered or gave a gratuity (e.g., an entertainment or gift) to an officer, official, or employee of the Central Purchasing Division of the Lead State.

9.12 Pricing

In accordance with 74 O.S. § 85.40, all travel expenses to be incurred by the Contractor in the performance of the Master Agreement shall be included in the total price/ amount.

.

9.13 Type of Contract

This is a firm fixed price contract for indefinite delivery and indefinite quantity for the supplies/services specified.

9.14 Open Records Act

Vendor acknowledges that all Oklahoma State agencies and certain other Oklahoma-based entities are subject to the Oklahoma Open Records Act. Vendor also acknowledges that such Customers will comply with the Oklahoma Open Records Act and with all opinions of the Oklahoma Attorney General concerning this Act. Except for a provision of the Contract specifically designated as confidential in a writing executed by both parties or a provision protected from disclosure in the Open Records Act, no Contract provision is confidential

information and, therefore, any provision is subject to disclosure under the Open Records Act.

9.15 . Patents and Copyrights

Without exception, a Product price shall include all royalties or costs owed by the Vendor to any third party arising from the use of a patent, intellectual property or copyright. Should any third party threaten or make a claim that any portion of a Product or Services provided by Vendor under the Contract infringes that party's patent or copyright, Vendor shall enable Customers to legally continue to use, or modify for use, the portion of the Product or Services at issue or replace such potentially infringing Product, or re-perform in the case of Services, with at least a functional non-infringing equivalent. Vendor's duty under this section shall extend to include other Products or Services rendered materially unusable as intended due to replacement or modification of the Products or Services at issue.

9.16 Compliance and Electronic and Information Technology Accessibility

Vendor shall comply with federal and State laws, rules and regulations related to information technology accessibility, as applicable, including but not limited to Oklahoma Information Technology Accessibility Standards ("Standards") set forth at http://www.ok.gov/cio/documents/isd-itas.pdf and shall provide a Voluntary Product Accessibility Template ("VPAT") describing such compliance, which may be provided via a URL linking to the VPAT. If Products require development or customization, additional requirements and documentation may be required and compliance shall be necessary by Vendor. Such requirements may be stated in appropriate documents including but not limited to a statement of work, riders, agreement, purchase order or Addendum. Accordingly, in each statement of work or similar document issued pursuant to the Contract, Vendor shall describe such compliance and identify, if and as applicable, (i) which exception to the Standards applies or (ii) a description of the tasks and estimated cost to make the proposed products and/or services compliant with applicable Standards.

9.17 Media Ownership (Disk Drive and/or Memory Chip Ownership)

Any disk drives and memory cards purchased with or included for use in leased or purchased Products under the Contract remain the property of the State or Customer, as applicable.

Personal information may be retained within electronic media devices and components; therefore, the State shall not allow the release of electronic media either between Customers or for the resale of refurbished equipment that has been in use by a Customer, by the Vendor to the general public or other entities. This provision applies to replacement devices and components, whether purchased or leased, supplied by Vendor, its agents or subcontractors during the downtime (repair) of Products purchased or leased through the Contract. If a device is removed from a location for repairs, the Customer shall have sole discretion, prior to removal, to determine and implement sufficient safeguards (such as a record of hard drive serial numbers) to protect personal information

that may be stored within the hard drive or memory of the device.

9.18 Offshore Services

No offshore services are provided for under the Contract. State data shall not be used or accessed internationally, for troubleshooting or any other use not specifically provided for herein without the prior written permission, which may be withheld in the State's sole discretion, from the appropriate authorized representative of the State.

9.19 High Technology System Performance and Upgrades

i. Pursuant to 62 O.S. § 34.12.1, if an Acquisition pursuant to the Contract includes a "high technology system" as defined at 62 O.S. 34.11.1(O) the Vendor shall provide documentation of the projected schedule of recommended or required system upgrades or improvements to such system for the three (3) year period following the purchase date. If Vendor does not plan such system upgrades or improvements, the Vendor shall provide documentation that no system upgrades or improvements to the high technology system are planned for the three (3) year period following the purchase date.

ii. Any Acquisition pursuant to the Contract of an upgrade or enhancement to a high technology system shall be conditioned upon one of the following: the Acquisition being provided at no charge to the State; the Acquisition being provided to the State at no additional charge pursuant to a previous agreement with the Vendor; the Vendor providing documentation that any required or recommended upgrade will enhance or is necessary for performance of the applicable State agency duties and responsibilities; or the Vendor providing documentation that it will no longer supply maintenance assistance to the applicable State agency and the applicable State agency documenting that the functions performed by the high technology system are necessary for performance of the State agency duties and responsibilities.

9.20 Emerging Technologies

The State of Oklahoma reserves the right to enter into an Addendum to the Contract at any time to allow for emerging technologies not identified elsewhere in the Contract Documents if there are repeated requests for such emerging technology or the State determines it is warranted to add such technology.

1. Double Click to Open PDF Fill able Form

MES

Vtl'AgATAtlgl

Responding Bidder Information

'Certification for Competitive Bid and Contract' MUST be submitted along with the response to the Solicitation.

1. RE: Solicitation _____

2. Bidder General Information:

FEI / SSN : _____ **VEN ID:** _____

Company Name: _____

3. Bidder Contact Information:

Address:

City: _____ **State:** **Zp Code:** _____

Contact Name: _____

Contact Title:

Ffione*. _____ **FAX#** _____

Email: _____ WeMite: _____

4. Oklahoma Sales Tax Permit':

- ❑ **YES - Permit *tt*** _____
- ❑ **NO - Exempt pursuant to Oklahoma Laws or Rules**

5. Registration with the Oklahoma Secretary of State:

- ❑ **YES - Filing Number.** _____
- ❑ **NO - Prior to the contract *award.* the successful bidder wit be required to register with the Secretary of State or must attach a signed statement that provides specific details supporting the exemption the supplier is claiming (lywer_sos ok oov or 405-521-3811).**

6. Workers' Compensation Insurance Coverage:

Bidder is required to provide with the bid a certificate of ĭ˝ism˝once showing proof of compliance with the Oklahoma Workers' Compensation Act

- ❑ **YES- include a certificate of insurance witi the bid**
- ❑ **NO - attach a signed statement that provides specific detail supporting the exemption you are claiming from the Workers' Compensation Act (Note: Pursuant to Attorney General Opinion #07-8. the exemption from 85 O.S. 2011. § 311 applies only to empbyers who are natural persons. such as note proprietors. and does not apply to employers who are entities created by law. including but not limited to corporations. partnerships and limited liability companies.)[2]**

Authorized Signature _____ **Date** _____

Printed Name _____ Tele _____

[1] For frequently asked questions concerning Oklafiorna Saes Tax Permit. see Dttonvfx **toxox** MITTIOLIMIOMMIeS 1da1(

For frequently **aS**ked questions concerning workers' compensation Insurance see ***=Plow*** OR oOMIOnos htmlef7/1

2. Double Click to Open Adobe Fill able Form

MMES

Certification for Competitive Bid
and/or Contract
(Non-Collusion Certification)

NOTE: A certikalion shag *be included weir any ,..unvedive bid and/or contract exceedng $5.000.00 subrnided to the Stale* ***for goods or services.***

Soicilation or Purchase Order #: _____

&corer Legal Name: _____

SECTION I [740.S. §135.22]:
A. For purposes of competitive bid.

1.1am the duly authorized agent of the above named bidder submiting the competitive bid herewith. for the purpose of certifythg the facts pertaining to the existence cf colusion among bidders and between bidders and state eficia/s **or employees. as wed as** facts **pertaining to the giring or offering of things of value to government personnel *in*** return for **special consideration in the lettng of any contract pursuant to said bid:**

2.1 an fully aware of tie fads and crownstarces arrounding the making of the bid to which this statemert is attached and have been personally and directly involved in the proceedings leading to the submission of such bid: and

3. **Neither the bidder nor anyone subject to the bidder's direction or coned has been a party:**

- **a. to any collusion among bidders in restraint of freedom of competion by .ikevviim it to bid a a fixed price or to retail from biding,**
- **b. to any allusion with any state offcial or employee as to quantity. quality or price in the prospedive co˙tract or as to *any* other terms of such pospective contact nor**
- **c. in any discussions between bidders and any state official concerning exchange of money or other thing of value for special consideration nine letting of a contract. nor**
- **0. to any collusion with any state agency or political subdivision official or employee as to create a sole-source acquisit¯ ion in contradiction to Section 85.441 of this tide.**

B. !certify. if awarded the contact, whether conthetitivey bid or not neither the contractor nor anyone subject to the contractor's direction a °ontol has paid, given or donated or agreed to pay. give or donate to any dhow or employee of tie State of Oklahoma any money or other thing of value. either 0 ready or thdrediy, in procuring this contract herein.

SECTION II [74 O.S.S **85.421:**
For the prpose of a contract for services. the supplier also certifies that no person who has been involved n any manner in the development of this contract while employed by the Stale of Oklahoma shall be employed by the supplier to fulfill **any of the services provided for under said =Urea**

The undersigned, duly authorized agent for the above named supplier, by signing below acknowledges this certification statement is executed for the purposes of:

1:1 the competitive bid attached herewith and contract, if awarded to said supplier;

OR

D **the contact attached heremth. which** was not :ompectlvely **bid and awarded by the agency pursuant to applicable Oklahoma stathtes.**

Suppler Autlonzed Sig ease	**Certified This Mee**
Printed Name	**Title**
Phone Number	**Email**
Fax Number	

01AES FORM CP DU -Rtschasing I Rev. 11/2015

10 . ATTACHMENT D – PRICING TEMPLATES

SEPARATE ATTACHMENT

10 ATTACHMENT E – ADMINISTRATIVE AND TECHNICAL RESPONSE TEMPLATE

SEPARATE ATTACHMENT

11 ATTACHMENT F – CJIS SECURITY POLICY V5.4

FEDERAL APPENDIX H SECURITY ADDENDUM

The following pages contain the legal authority, purpose, and genesis of the Criminal Justice Information Services Security Addendum (H2-H4); the Security Addendum itself (H5-H6); and the Security Addendum Certification page (H7).

FEDERAL BUREAU OF INVESTIGATION

CRIMINAL JUSTICE INFORMATION SERVICES SECURITY ADDENDUM

Legal Authority for and Purpose and Genesis of the Security Addendum

Traditionally, law enforcement and other criminal justice agencies have been responsible for the confidentiality of their information. Accordingly, until mid-1999, the Code of Federal Regulations Title 28, Part 20, subpart C, and the National Crime Information Center (NCIC) policy paper approved December 6, 1982, required that the management and exchange of criminal justice information be performed by a criminal justice agency or, in certain circumstances, by a noncriminal justice agency under the management control of a criminal justice agency.

In light of the increasing desire of governmental agencies to contract with private entities to perform administration of criminal justice functions, the FBI sought and obtained approval from the United States Department of Justice (DOJ) to permit such privatization of traditional law enforcement functions under certain controlled circumstances. In the Federal Register of May 10, 1999, the FBI published a Notice of Proposed Rulemaking, announcing as follows:

> 1. Access to CHRI [Criminal History Record Information] and Related Information, Subject to Appropriate Controls, by a Private Contractor Pursuant to a Specific Agreement with an Authorized Governmental Agency To Perform an Administration of Criminal Justice Function (Privatization). Section 534 of title 28 of the United States Code authorizes the Attorney General to exchange identification, criminal identification, crime, and other records for the official use of authorized officials of the federal government, the states, cities, and penal and other institutions. This statute also provides, however, that such exchanges are subject to cancellation if dissemination is made outside the receiving departments or related agencies. Agencies authorized access to CHRI traditionally have been hesitant to disclose that information, even in furtherance of authorized criminal justice functions, to anyone other than actual agency employees lest such disclosure be viewed as unauthorized. In recent years, however, governmental agencies seeking greater efficiency and economy have become increasingly interested in obtaining support services for the administration of criminal justice from the private sector. With the concurrence of the FBI's Criminal Justice Information Services (CJIS) Advisory Policy Board, the DOJ has concluded that disclosures to private persons and entities providing support services for criminal justice agencies may, when subject to appropriate controls, properly be viewed as permissible disclosures for purposes of compliance with 28 U.S.C. 534.
>
> We are therefore proposing to revise 28 CFR 20.33(a)(7) to provide express authority for such arrangements. The proposed authority is similar to the authority that already exists in 28 CFR 20.21(b)(3) for state and local CHRI systems. Provision of CHRI under this authority would only be permitted pursuant to a specific agreement with an authorized governmental agency for the purpose of providing services for the administration of criminal justice. The agreement would be required to incorporate a security addendum approved

by the Director of the FBI (acting for the Attorney General). The security addendum would specifically authorize access to CHRI, limit the use of the information to the specific purposes for which it is being provided, ensure the security and confidentiality of the information consistent with applicable laws and regulations, provide for sanctions, and contain such other provisions as the Director of the FBI (acting for the Attorney General) may require. The security addendum, buttressed by ongoing audit programs of both the FBI and the sponsoring governmental agency, will provide an appropriate balance between the benefits of privatization, protection of individual privacy interests, and preservation of the security of the FBI's CHRI systems.

The FBI will develop a security addendum to be made available to interested governmental agencies. We anticipate that the security addendum will include physical and personnel security constraints historically required by NCIC security practices and other programmatic requirements, together with personal integrity and electronic security provisions comparable to those in NCIC User Agreements between the FBI and criminal justice agencies, and in existing Management Control Agreements between criminal justice agencies and noncriminal justice governmental entities. The security addendum will make clear that access to CHRI will be limited to those officers and employees of the private contractor or its subcontractor who require the information to properly perform services for the sponsoring governmental agency, and that the service provider may not access, modify, use, or disseminate such information for inconsistent or unauthorized purposes.

Consistent with such intent, Title 28 of the Code of Federal Regulations (C.F.R.) was amended to read:

§ 20.33 Dissemination of criminal history record information.

a) Criminal history record information contained in the Interstate Identification Index (III) System and the Fingerprint Identification Records System (FIRS) may be made available:

1) To criminal justice agencies for criminal justice purposes, which purposes include the screening of employees or applicants for employment hired by criminal justice agencies.

2) To noncriminal justice governmental agencies performing criminal justice dispatching functions or data processing/information services for criminal justice agencies; and

3) To private contractors pursuant to a specific agreement with an agency identified in paragraphs (a)(1) or (a)(6) of this section and for the purpose of providing services for the administration of criminal justice pursuant to that agreement. The agreement must incorporate a security addendum approved by the Attorney General of the United States, which shall specifically authorize access to criminal history record information, limit the use of the information to the purposes for which it is provided, ensure the security and confidentiality of the information consistent with these regulations, provide for sanctions, and contain

such other provisions as the Attorney General may require. The power and authority of the Attorney General hereunder shall be exercised by the FBI Director (or the Director's designee).

This Security Addendum, appended to and incorporated by reference in a government-private sector contract entered into for such purpose, is intended to insure that the benefits of privatization are not attained with any accompanying degradation in the security of the national system of criminal records accessed by the contracting private party. This Security Addendum addresses both concerns for personal integrity and electronic security which have been addressed in previously executed user agreements and management control agreements.

A government agency may privatize functions traditionally performed by criminal justice agencies (or noncriminal justice agencies acting under a management control agreement), subject to the terms of this Security Addendum. If privatized, access by a private contractor's personnel to NCIC data and other CJIS information is restricted to only that necessary to perform the privatized tasks consistent with the government agency's function and the focus of the contract. If privatized the contractor may not access, modify, use or disseminate such data in any manner not expressly authorized by the government agency in consultation with the FBI.

FEDERAL BUREAU OF INVESTIGATION

CRIMINAL JUSTICE INFORMATION SERVICES SECURITY

ADDENDUM

The goal of this document is to augment the CJIS Security Policy to ensure adequate security is provided for criminal justice systems while (1) under the control or management of a private entity or (2) connectivity to FBI CJIS Systems has been provided to a private entity (contractor). Adequate security is defined in Office of Management and Budget Circular A- 130 as "security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information."

The intent of this Security Addendum is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

This Security Addendum identifies the duties and responsibilities with respect to the installation and maintenance of adequate internal controls within the contractual relationship so that the security and integrity of the FBI's information resources are not compromised. The security program shall include consideration of personnel security, site security, system security, and data security, and technical security.

The provisions of this Security Addendum apply to all personnel, systems, networks and support facilities supporting and/or acting on behalf of the government agency.

1.0 Definitions

1.01 Contracting Government Agency (CGA) - the government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor subject to this Security Addendum.

1.02 Contractor - a private business, organization or individual which has entered into an agreement for the administration of criminal justice with a Criminal Justice Agency or a Noncriminal Justice Agency.

2.00 Responsibilities of the Contracting Government Agency.

2.01 The CGA will ensure that each Contractor employee receives a copy of the Security Addendum and the CJIS Security Policy and executes an acknowledgment of such receipt and the contents of the Security Addendum. The signed acknowledgments shall remain in the possession of the CGA and available for audit purposes. The acknowledgement may be signed by hand or via digital signature (see glossary for definition of digital signature).

3.0 Responsibilities of the Contractor.

3.01 The Contractor will maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed and all subsequent versions), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

4.00 Security Violations.

4.01 The CGA must report security violations to the CJIS Systems Officer (CSO) and the Director, FBI, along with indications of actions taken by the CGA and Contractor.

4.02 Security violations can justify termination of the appended agreement.

4.03 Upon notification, the FBI reserves the right to:

a. Investigate or decline to investigate any report of unauthorized use;

b. Suspend or terminate access and services, including telecommunications links. The FBI will provide the CSO with timely written notice of the suspension. Access and services will be reinstated only after satisfactory assurances have been provided to the FBI by the CGA and Contractor. Upon termination, the Contractor's records containing CHRI must be deleted or returned to the CGA.

5.00 Audit

5.01 The FBI is authorized to perform a final audit of the Contractor's systems after termination of the Security Addendum.

6.00 Scope and Authority

6.01 This Security Addendum does not confer, grant, or authorize any rights, privileges, or obligations on any persons other than the Contractor, CGA, CJA (where applicable), CSA, and FBI.

6.02 The following documents are incorporated by reference and made part of this agreement: (1) the Security Addendum; (2) the NCIC 2000 Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20. The parties are also subject to applicable federal and state laws and regulations.

6.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they augment the provisions of the CJIS Security Policy to provide a minimum basis for the security of the system and contained information and it is understood that there may be terms and conditions of the appended Agreement which impose more stringent requirements upon the Contractor.

6.04 This Security Addendum may only be modified by the FBI, and may not be modified by the parties to the appended Agreement without the consent of the FBI.

6.05 All notices and correspondence shall be forwarded by First Class mail to:

Information Security Officer

Criminal Justice Information Services Division, FBI 1000 Custer

Hollow Road

Clarksburg, West Virginia 26306

FEDERAL BUREAU OF INVESTIGATION

CRIMINAL JUSTICE INFORMATION SERVICES SECURITY

ADDENDUM

CERTIFICATION

I hereby certify that I am familiar with the contents of (1) the Security Addendum, including its legal authority and purpose; (2) the NCIC Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20, and agree to be bound by their provisions.

I recognize that criminal history record information and related data, by its very nature, is sensitive and has potential for great harm if misused. I acknowledge that access to criminal history record information and related data is therefore limited to the purpose(s) for which a government agency has entered into the contract incorporating this Security Addendum. I understand that misuse of the system by, among other things: accessing it without authorization; accessing it by exceeding authorization; accessing it for an improper purpose; using, disseminating or re-disseminating information received as a result of this contract for a purpose other than that envisioned by the contract, may subject me to administrative and criminal penalties. I understand that accessing the system for an appropriate purpose and then using, disseminating or re-disseminating the information received for another purpose other than execution of the contract also constitutes misuse. I further understand that the occurrence of misuse does not depend upon whether or not I receive additional compensation for such authorized activity. Such exposure for misuse includes, but is not limited to, suspension or loss of employment and prosecution for state and federal crimes.

_____ _____

Printed Name/Signature of Contractor Employee Date

_____ _____

Printed Name/Signature of Contractor Representative Date

_____

Organization and Title of Contractor Representative

12 ATTACHMENT G – REFERENCE TEMPLATE

Survey Questionnaire – State of Oklahoma

To: _____

(Name of person completing survey)

Phone: _____ Email: _____

Subject: Past Performance Survey of: _____

(Name of Vendor)

The State of Oklahoma in partnership with NASPO ValuePoint is implementing a process that collects past performance information on firms and their key personnel. The information will be used to assist the State(s) in the selection of firms to perform various projects. The firm/individual listed above has listed you as a client for which they have previously done business.

We would appreciate your taking the time to complete this survey.

Rate each of the criteria on a scale of 1 to 10, with 10 representing that you were very satisfied (and would hire the firm/individual again) and 1 representing that you were very unsatisfied (and would never hire the firm/individual again). Please rate each of the criteria to the best of your knowledge. If you do not have sufficient knowledge of past performance in a particular area, leave it blank.

Once complete, please send the form directly to the Vendor so they may submit the results with their response to our current Request for Proposal.

Client Name: _____ Completion Date: _____

Project Name: _____

Survey Questionnaire – State of Oklahoma

NO	CRITERIA	UNIT	
1	How would you rate the supplier's product availability and fill rate?	(1-10)	
2	How would you rate the experience of the supplier in managing large accounts?	(1-10)	
3	How would you rate the performance of suppliers products compare to that of its competitors?	(1-10)	
4	How would rate the suppliers turnaround time when contacted to provide information?	(1-10)	
5	How would you rate the suppliers ordering system?	(1-10)	
6	How would you rate the supplier's geographic coverage and ability to deliver throughout all your locations?	(1-10)	
7	How would you rate supplier's accounts receivable/invoice procedures?	(1-10)	
8	How would you rate suppliers post sales customer relations (Training, Technical Support, and Assistance)?	(1-10)	
9	Overall customer satisfaction and comfort level in hiring vendor/individual again	(1-10)	

Please list any additional comments you may have in the space provided below.

Printed Name (of Evaluator)		Signature (of Evaluator)

Thank you for your time and effort in assisting the State of Oklahoma in this important endeavor.

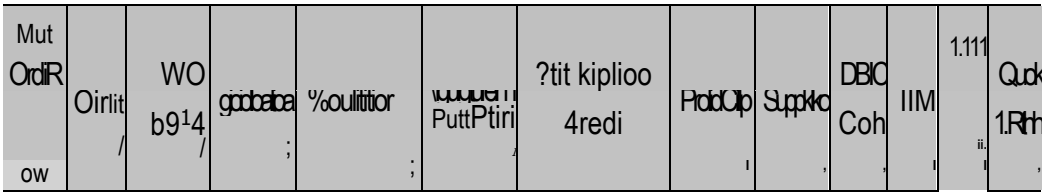
13 ATTACHMENT H – QUESTION TEMPLATE

Separate Attachment

14 ATTACHMENT I – USAGE REPORTING TEMPLATE EXAMPLE

Upon award all suppliers will receive template in excel format.

3.) field Descriptions



Mut OrdlR ow	Oirlit /	WO b9[1]4 /	gpdbatica ;	%oulittior ;	PuttPtiri	?tit kiplioo 4redi	ProbdOp	SuppKko	DBIC Coh	IIM	1.111 ii.	Quck 1.Rth

A I (0 1

kEnter the Ordering Entity's Purchase Order number, if it IS 0 P-OCrd purchase, 1) 1E3 enter "REP in the cel. **Do** not enter the credit card number.

B. Riff the date the order was placed.

C. Enter the Purchasing EPltp Sname, abbreviation, or number here. To identify State Agencies or Higher Education institutions, please reference the 'Abbreviation List tab at the bottom of the workbook.

D. Enter the city M which products or services were received, or the pe Ot C of fe sub division title (i.e, MC Mable Basset).

E. Enter the Products Manufacturer. If this a service, indicate the he type of service (Translation, Consulting,

P[09[011111119, etc.). Enter the Manufacturer Item Number, if applicable.

G. The Product Description should concisely explain what has been received by the end user

H. General Product Category, if applicable.

I. Enter the Supplier Item Number, if applicable.

J. The UNSPSC Codes CCP he found at the website listed above by 81181111 19 a key word in the "Search Title" field.

www.unspsc.org/search code

K. Enter the MSRP or list Price.

L Enter the price received by the Purchasing Entity.

M. Enter the Quantity purchased.

Remaining fields will automatically *calculate based* on the values entered.

Attachment J
Value Added Plan

This template must be used. The Value Added Plan should identify any value added options or ideas that may benefit the State(s). The value added claims should be prioritized (identify the most important claims first). The Respondent may add or delete Value Added Claim table templates, but do not exceed the 2-page limit for this section. Do NOT include any identifying information in the Plan. Information listed under the "Documented Performance" line may describe where the Respondent has used the approach or solution previously, and what the results were in terms of verifiable metrics.

Example (this example can be deleted to accommodate more claims)

Item Claim: *This would be the place to offer service/package/optional remittance method (etc) not requested in the solicitation-insert description here*

How will this add value? *How would the item described above add value to the State's contract?*

Documented Performance: *State in general terms where offered and the results*

Cost Impact: *What is cost or hourly rate?* ***Schedule Impact :*** *What is the unit of measure for the cost?*

Item #1 Claim:

How will this add value?

Documented Performance:

Cost Impact: **Schedule Impact:**

Item #2 Claim:

How will this add value?

Documented Performance:

Cost Impact: **Schedule Impact:**

Item #3 Claim:

How will this add value?

Documented Performance:

Cost Impact: **Schedule Impact:**

Item #4 Claim:

How will this add value?

Documented Performance:

Cost Impact: **Schedule Impact:**

Item #5 Claim:

How will this add value?

Documented Performance:

Cost Impact: **Schedule Impact:**

16 ATTACHMENT K – ADDITIONAL STATE TERMS AND CONDITIONS

STATE OF MONTANA

ADDITIONAL TERMS

The State of Montana (State) would like the following clauses included in the final contract(s). In instances where there are contradictory statements, the language herein shall dictate.

ACCESS AND RETENTION OF RECORDS: Contractor shall provide the State, Legislative Auditor, or their authorized agents' access to any records necessary to determine contract compliance. (18- 1-118, MCA.)

ASSIGNMENT, TRANSFER, AND SUBCONTRACTING: Contractor may not assign; transfer, or subcontract any portion of this contract without the State' prior written consent. (18-4-141, MCA.)

COMPLIANCE WITH LAWS: Contractor shall, in performance of work under this contract, fully comply with all applicable federal, state, or local laws, rules, and regulations, including but not limited to, the Montana Human Rights Act, the Civil Rights Act of 1964, the Age Discrimination Act of 1975, the Americans with Disabilities Act of 1990, and Section 504 of the Rehabilitation Act of 1973. Any subletting or subcontracting by Contractor subjects subcontractors to the same provision. In accordance with 49-3-207, MCA, Contractor agrees that the hiring of persons to perform this contract will be made on the basis of merit and qualifications and there will be no discrimination based upon race, color, religion, creed, political ideas, sex, age, marital status, physical or mental disability, or national origin by the persons performing this contract.

CHOICE OF LAW AND VENUE: Montana law governs this contract. The parties agree that any litigation concerning this bid, proposal, or subsequent contract must be brought in the First Judicial District in and for the County of Lewis and Clark, State of Montana, and each party shall pay its own costs and attorney fees. (18-1-401, MCA.)

HOLD HARMLESS/INDEMNIFICATION: Contractor agrees to protect, defend, and save the State, its elected and appointed officials, agents, and employees, while acting within the scope of their duties as such, harmless from and against all claims, demands, causes of action of any kind or character, including the cost of defense thereof, arising in favor of Contractor's employees or third parties on account of bodily or personal injuries, death, or damage to property arising out of services performed or omissions of services or in any way resulting from the acts or omissions of Contractor and/or its agents, employees, representatives, assigns, subcontractors, except the sole negligence of the State, under this agreement.

REDUCTION OF FUNDING: The State must terminate this contract if funds are not appropriated or otherwise made available to support the State's continuation of performance of this contract in a subsequent fiscal period. (18-4-313(4), MCA.) If state or federal government funds are not appropriated or otherwise made available through the state budgeting process to support continued performance of this contract (whether at an initial contract payment level or any contract increases to that initial level) in subsequent fiscal periods, the State shall terminate this contract as required by law. The State shall provide Contractor the date the State's termination shall take effect. The State shall not be liable to Contractor for any payment that would have been payable had the contract not been terminated under this provision. As stated above, the State shall be liable to Contractor only for the payment, or prorated portion of that payment, owed to Contractor up to the date the State's termination takes effect. This is Contractor's sole remedy. The State shall not be liable to Contractor for any other payments or damages arising from termination under this section, including but not limited to general, special, or consequential damages such as lost profits or revenues.

17 ATTACHMENT L – ADDITIONAL STATE TERMS AND CONDITIONS

STATE OF VIRGINIA

A. PURPOSE

The purpose of this Intent to Participate agreement ("ITP") is to provide members of the National Association of State Procurement Officials ("NASPO") with the opportunity to participate in multi-state cooperative contract(s) for the provision of Public Safety / Law Enforcement Video & Vehicular Mounted Equipment for Participating States, including all related integral and peripheral component materials and parts, and all related Services. These contract(s) are being led by the State of Oklahoma ("Lead State").

B. SCOPE OF THE CONTRACT(S)

The Lead State is authorized by the Commonwealth as a Participating State, through this ITP, and the NASPO Cooperative Purchasing Organization to act as the lead procurement officer in developing one or more multi-state cooperative contracts for Public Safety Video Systems & Services. The resulting contracts will be permissive contracts.

It is the intent of the Commonwealth of Virginia to participate in this joint procurement for Public Safety Video Systems & Services through NASPO in order to obtain most optimal cost savings and/or reductions in administrative expense for the Commonwealth and its Public Bodies.

Subject to the participation by the Virginia Department of General Services ("DGS"), any subsequent contract that may be awarded as a result of this RFP will be made available for use by all Commonwealth of Virginia state agencies, institutions, or any other public body, as defined in § 2.2-4301 entitled "Definitions" and § 2.2-4304 entitled "Joint and cooperative procurement" of the Virginia Public Procurement Act (VPPA). Further, any such contracts resulting from this RFP may also be made available for use by certain charitable corporations and private nonprofit 501(c)(3) institutions of higher education that are chartered in Virginia, as allowable pursuant to Virginia Code 2.2-1120. Collectively, all aforementioned Commonwealth parties are referred to hereinafter in the aggregate as "Authorized Users".

To ensure maximum transparency and public access to the Commonwealth's procurement activities and opportunities, and consistent with Virginia Code § 2.2-1110, all Authorized Users shall be required to submit all orders directly with a contractor through the Commonwealth's central electronic procurement website, and details for this will be delineated in any subsequently negotiated ordering instructions of the Commonwealth's Participating Addendum.

Administrative Fee

A NASPO administrative fee of one-quarter of one percent (0.25%) will be assessed centrally for purchases under the contract.

The Commonwealth's administrative fee/s, if any, and the detailed processes for managing, administering, and recording such fee payments shall be added at such time that a Participating Addendum may be executed by the Commonwealth.

The Commonwealth of Virginia requires the use of certain contractual terms and conditions, delineated below, and it will add any other terms and conditions needed at the appropriate time that any Participating Addendum ("PA") may be negotiated.

C. TERM OF THE CONTRACT

The initial term of this Master Agreement is for two (2) years. This Master Agreement may be extended beyond the original contract period for three (3) additional years at the Lead State's discretion and by mutual agreement and upon review of requirements of Participating Entities, current market conditions, and Contractor performance.

D. SOLICITATION AND CONTRACT DEVELOPMENT/ADDITIONAL INFORMATION

The solicitation and contract development shall be accomplished in compliance with the NASPO ValuePoint Process Guide and the NASPO Memorandum of Agreement for the NASPO cooperative purchasing program, incorporated herein by reference.

Proposal Due Date:

Proposals must be received by June 20, 2016 3:00 PM CDT, or as otherwise detailed in the most recent relevant RFP or Amendment documents issued by the Lead State. Proposals received after any such deadline will be late, and ineligible for consideration.

Solicitation Type and Evaluation Criteria

The RFP will be issued and evaluated in accordance with the NASPO Cooperative Purchasing Organization guidance, and the procurement laws and rules of the Lead State by a sourcing team composed of members from several states.

Award(s): The solicitation will permit multiple awards.

The following contractual terms and conditions shall be applicable to any Offeror and Virginia's participation in this joint or cooperative procurement conducted by another state:

1. VIRGINIA PUBLIC PROCUREMENT ACT

The Virginia Public Procurement Act ("VPPA", § 2.2-4300 et seq. of the Code of Virginia), including Article 6 (*Ethics in Public Contracting*), shall apply to any contract entered into between a vendor and a Virginia public body under this solicitation.

2. AUTHORIZATION TO CONDUCT BUSINESS IN THE COMMONWEALTH

A contractor organized as a stock or nonstock corporation, limited liability company, business trust, or limited partnership or registered as a limited liability partnership shall be authorized to transact business in the Commonwealth as a domestic or foreign

business entity if so required by Title 13.1 or Title 50 of the Code of Virginia or as otherwise required by law. Any business entity described above that enters into a contract with a public body shall not allow its existence to lapse or its certificate of authority or registration to transact business in the Commonwealth, if so required under Title 13.1 or Title 50, to be revoked or cancelled at any time during the term of the contract. A public body may void any contract with a business entity if the business entity fails to remain in compliance with the provisions of this section, in addition to any other available remedy.

3. NON-DISCRIMINATION

a. During the performance of this contract, the contractor agrees as follows:

i. The contractor will not discriminate against any employee or applicant for employment because of race, religion, color, sex, national origin, age, disability, or other basis prohibited by state law relating to discrimination in employment, except where there is a bona fide occupational qualification reasonably necessary to the normal operation of the contractor. The contractor agrees to post in conspicuous places, available to employees and applicants for employment, notices setting forth the provisions of this nondiscrimination clause.

ii. The contractor, in all solicitations or advertisements for employees placed by or on behalf of the contractor, will state that such contractor is an equal opportunity employer.

iii. Notices, advertisements and solicitations placed in accordance with federal law, rule or regulation shall be deemed sufficient for the purpose of meeting the requirements of this section.

b. The contractor will include the provisions of the foregoing paragraphs i, ii and iii in every subcontract or purchase order of over $10,000, so that the provisions will be binding upon each subcontractor or vendor.

c. In accordance with Section 2.2-4343 of the Code of Virginia, public bodies do not discriminate against faith-based organizations, , or against any bidder or offeror because of race, religion, color, sex, national origin, age, disability, or any other basis prohibited by Virginia law.

4. IMMIGRATION REFORM AND CONTROL ACT OF 1986

By entering into a written contract with the Commonwealth of Virginia, the contractor certifies that it does not, and shall not, during the performance of this contract, knowingly employ an unauthorized alien as defined in the federal Immigration Reform and Control Act of 1986.

5. DEBARMENT STATUS

By participating in this contract, the contractor certifies that it is not currently debarred by the Commonwealth of Virginia from submitting a response for the type of goods or services covered by this contract. The contractor further certifies that it is not debarred from filling any order or accepting any resulting order, and that it is not an agent of any person or entity that is currently debarred by the Commonwealth of Virginia.

6. DRUG-FREE WORKPLACE

During the performance of this contract, the contractor agrees to:

a. provide a drug-free workplace for its employees;

b. post in conspicuous places, available to employees and applicants for employment, a statement notifying employees that the unlawful manufacture, sale, distribution, dispensation, possession, or use of a controlled substance or marijuana is prohibited in the contractor's workplace and specifying the actions that will be taken against employees for violations of such prohibition;

c. state in all solicitations or advertisements for employees placed by or on behalf of the contractor that the contractor maintains a drug-free workplace; and

d. include the provisions of the foregoing clauses in every subcontract or purchase order of over $10,000, so that the provisions will be binding upon each subcontractor.

e. For the purposes of this section, "drug-free workplace" means a site for the performance of work done in connection with a specific contract awarded to a contractor, the employees of whom are prohibited from engaging in the unlawful manufacture, sale, distribution, dispensation, possession or use of any controlled substance or marijuana during the performance of the contract.

7. ASSIGNMENT OF CONTRACT

Contracts and purchase orders with Virginia agencies shall not be assignable by the contractor in whole or in part without the written consent of that agency.

8. eVA BUSINESS-TO-GOVERNMENT VENDOR REGISTRATION, CONTRACTS, AND ORDERS

All contractors providing goods or services to the Commonwealth of Virginia shall participate in the eVA Internet e-procurement solution by completing the free eVA Vendor Registration located online at www.eva.virginia.gov. All contractors must register in eVA and pay the Vendor Transaction Fees specified below before they may fulfill any order. Vendor transaction fees are determined by the current fees, as follows:

a. DSBSD-certified Small Businesses*: 1%, capped at $500 per order.

b. Businesses that are not DSBSD-certified Small Businesses: 1%, capped at $1,500 per order.

* Virginia Department of Small Business and Supplier Development, http://www.sbs d.virginia.gov/

9. PAYMENT

a. To Prime Contractor:

i. Contractor shall submit invoices for items ordered, delivered and accepted directly to the payment address shown on the purchase order or contract. All invoices shall show the state contract number, purchase order number, and social security number (for individual contractors) or federal employer identification number (for proprietorships, partnerships, and corporations).

ii. Any payment terms requiring payment in less than 30 days will be regarded as requiring payment 30 days after invoice or delivery, whichever occurs last. This shall not affect offers of discounts for payment in less than 30 days, however.

iii. All goods or services provided under this contract or purchase order, that are to be paid for with public funds, shall be billed by the contractor at the contract price, regardless of which public agency is being billed.

iv. The following shall be deemed to be the date of payment: the date of postmark in all cases where payment is made by mail, or the date of offset when offset proceedings have been instituted as authorized under the Virginia Debt Collection Act.

v. Unreasonable Charges. Under certain emergency procurements and for most time and material purchases, final job costs cannot be accurately determined at the time orders are placed. In such cases, final payment in full is contingent on a determination that all invoiced charges are reasonable. Charges which appear to be unreasonable will be researched and challenged, and that portion of the invoice held in abeyance until a settlement can be reached. Upon determining that invoiced charges are not reasonable, the Commonwealth shall promptly notify the contractor, in writing, as to those charges which it considers unreasonable and the basis for the determination. A contractor may not institute legal action unless a settlement cannot be reached within thirty (30) days of notification. The provisions of this section do not relieve an agency of its prompt payment obligations with respect to those charges that are not in dispute (Code of Virginia, § 2.2-4363).

b. To Subcontractors:

i. A contractor awarded a contract under this solicitation is hereby obligated to pay the subcontractors within seven days of the contractor's receipt of payment from the Commonwealth for the proportionate share of the payment received for work performed by the subcontractors under the contract; or to notify the agency and the subcontractors, in writing, of the contractor's intention to withhold payment and the reason.

ii. The contractor is obligated to pay the subcontractors interest at the rate of one percent per month (unless otherwise provided in this contract) on all amounts owed by the contractor that remain unpaid seven days following receipt of payment from the Commonwealth, except for amounts withheld as stated in (i) above. The date of mailing of any payment by U. S. Mail is deemed to be payment to the addressee. These provisions apply to each sub-tier contractor performing under the primary contract. A contractor's obligation to pay an interest charge to a subcontractor may not be construed to be an obligation of the Commonwealth.

10. MODIFICATIONS

This contract may be modified in accordance with §2.2-4309 of the Code of Virginia. No modifications shall be effective unless it is in writing and signed by the duly authorized representative of the Commonwealth. No term or provision hereof shall be deemed waived and no breach excused unless such waiver or consent to breach is in writing. Any contract issued on a firm fixed price basis may not be increased more than twenty five percent (25%) or
$50,000.00 whichever is greater, without the approval of the Governor or his authorized designee. In no event may the amount of the contract be increased without adequate consideration. The unauthorized approval of a modification cannot be the basis of a contractual claim as set forth in § 2.2-4363.

11. APPLICABLE LAWS AND COURTS

This contract shall be governed in all respects by the laws of the Commonwealth of Virginia, without reference to its choice of law rules. Any litigation involving a Virginia public body shall be brought in the Circuit Court for the City of Richmond. The contractor shall comply with all applicable federal, state and local laws, rules and regulations.

12. VENDORS MANUAL

This solicitation is subject to the provisions of the Commonwealth of Virginia Vendors Manual and any changes or revisions thereto, which are hereby incorporated into this contract in their entirety. The procedure for filing contractual claims is in section 7.19 of the Vendors Manual. A copy of the Vendors Manual is available for review at the purchasing office and is also accessible on the Internet at www.eva.virginia.gov under the "I Sell to Virginia" tab.

13. ALTERNATIVE DISPUTE RESOLUTION

The Commonwealth or any Authorized User and the contractor are encouraged to resolve any issues in controversy arising from the award of the contract or any contractual dispute using Alternative Dispute Resolution (ADR) procedures (Code of Virginia, § 2.24366). ADR procedures are described in Chapter 9 of the Vendors Manual.

14. ETHICS IN PUBLIC CONTRACTING

By fulfilling an order placed by a Virginia buyer, the contractor certifies that they have not engaged in collusion or fraud in relation to any aspect of this contract, or its contract with the lead state or other entity that conducted the procurement upon which this contract is based, and that it has not offered or received any kickbacks or inducements to or from any other bidder, offeror, supplier, manufacturer, or subcontractor in connection with this contract or procurement. The contractor also certifies that it has not conferred on any public employee having responsibility for this procurement transaction any payment, loan, subscription, advance, deposit of money, services or anything of more than nominal value, present or promised, unless consideration of substantially equal or greater value was exchanged.

15. SECURITY REQUIREMENTS – VIRGINIA INFORMATION TECHNOLOGIES AGENCY ("VITA")

As applicable, Contractor certifies and warrants that all Products and Services provided pursuant to the Agreement shall conform to all applicable federal, state and local laws and regulations governing data security and the operations that govern these Products and Services. Such conformance specifically includes the Information and Data Security Policies, Standards, and Guidelines issued by the Commonwealth through the Virginia Information Technologies Agency (VITA) as delineated at the following, or any then-current, URL: http://www.vita.virginia.gov/default.as px?id=537 or any other information technology or Sensitive Data security requirements established by VITA and pertinent to the Products and Services.

Should an Authorized User have or establish additional security procedures pertinent to

the Products or Services, then Contractor agrees to work with the Authorized User to ensure that Products or Services also conform to such requirements, as may be mutually agreeable between the Authorized User and the Contractor.

For any individual Authorized User location, security procedures may include, but not be limited to: background checks, records verification, photographing, and fingerprinting of Contractor's employees or agents. Contractor may, at any time, be required to execute and complete, for each individual Contractor employee or agent, additional forms which may include non- disclosure agreements to be signed by Contractor's employees or agents acknowledging that all Authorized User information with which such employees and agents come into contact while at the Authorized User site is confidential and proprietary. Any unauthorized release of confidential or Personal information by the Contractor or an employee or agent of Contractor shall constitute a breach of its obligations under this Section and the Contract.

Contractor shall immediately notify DGS and VITA points-of-contact (to be included at a later date), and the Authorized User point-of-contact identified in any Order, of any Breach of Unencrypted and Unredacted Personal Information, as those terms are defined in Virginia Code 18.2-186.6, or any other Sensitive Information, as defined herein and including, but not limited to, insurance data, social security number, date of birth, etc., which may be collected in the performance of the Contractor's Products or Services under this Agreement, or as may be provided to the Contractor by the Commonwealth or any Authorized User. Contractor shall provide the Commonwealth, through VITA, or any Authorized User, as applicable, with the opportunity to participate in the investigation of the Breach and to exercise control over reporting the unauthorized disclosure, to the extent permitted by law.

Contractor shall indemnify, defend, and hold the Commonwealth, DGS, VITA, the Authorized User, or their officers, directors, employees and agents harmless from and against any and all fines, penalties (whether criminal or civil), judgments, damages and assessments, including reasonable expenses suffered by, accrued against, or charged to or recoverable from the Commonwealth, DGS, VITA, the Authorized User, or their officers, directors, agents or employees, on account of the failure of Contractor to perform its obligations pursuant this Section.

To the extent applicable, and for any Contractor Services that may be agreed upon to be provided through any separate license agreement (Licensed Services), VITA shall have the opportunity and right to review Contractor's information security program prior to the commencement of such Licensed Services, and from time-to-time during the term of this Agreement.

During the performance of any such Licensed Services, and on an ongoing basis from time-to- time, VITA, at its own expense, shall be entitled to perform, or to have performed, an on-site audit of Contractor's information security program. In lieu of an on-site audit, and upon the request by VITA, Contractor agrees to complete, within forty-five (45 days) of receipt, an audit questionnaire provided by VITA regarding the Contractor's information security program. Contractor agrees that they shall implement any reasonably required safeguards as identified by any VITA information security program audit.

THE COMMONWEALTH RESERVES THE RIGHT TO NEGOTIATE ANY ADDITIONAL REQUIRED CONTRACTUAL PROVISIONS AT SUCH TIME THAT ANY PARTICIPATING ADDENDUM MAY BE EXECUTED, IF ANY.

Oklahoma/NASPO ValuePoint
OK-MA-145 - Public Safety Video and Vehicle Mounted Equipment
Attachment E: Administrative and Technical Proposal Response Template

Business Proposal
Respondent Name: COBAN Technologies, Inc.

Instructions:
Fill out the yellow shaded areas only. Blank cells will be considered as "No Response."
This appendix contains questions related to general Proposer Information. The information provided by Proposers will be used in the qualitative portions of the evaluation process.

1. General Questions and Proposer Stability

1. Provide the name, title, street address, city, state, zip code, e-mail address, fax and telephone numbers

Name of Primary Contact	Larry Marr
Title	National Technical Sales Support
Address	11375 W Sam Houston Pkwy, Suite 800
City	Houston
State	Texas
Zip Code	77031
Email Address	pmo@cobantech.com
Telephone	281-925-0488
Fax	281-925-0535
Mobile	713-502-7589

2. Please provide all of the following corporate information.

Main Line Of Business:	In-Car Video Systems and Body Worn Cameras
# of years in business:	14 years
# of employees:	80
Name of Parent Company, if any:	N/A
Name of Subsidiaries, if any:	N/A

3. Is your firm's primary line of business video or vehicle equipment sales? Indicate with an "X" below:

Yes	X	No	

Are there other related lines of business that your firm participates in? If so, please list and describe.

In Car video, Body worn Cameras, IP interview room, video storage and management.

4. Provide an overview of your business model. As a manufacturer, how would you distribute products; direct ship or distributors? If using authorized distributors, please provide listing

COBAN is a direct to customer manufacturer. We do not use distributors or channel partners to sell our product lines.

5. Provide an overview of the geographical locations of the firm at the national, regional, and local levels.

COBAN is Headquartered in Houston, Texas and has numerous Field Engineers, Regional Sales Managers, and Inside Sales Managers that are assigned territories across the United States. COBAN's Technical Support Call center is based in Houston as well. COBAN covers and supports all 50 states.

6. Are major changes (acquisitions, re-structuring, alliances, joint ventures) taking place in your organization? Please provide your answer as succinctly as possible since we are only asking for very critical issues that might significantly impact our evaluation of your company/proposal.

No, at this time there are no acquisitions, re-structures or joint ventures being planned. COBAN manufactures, distributes, and supports their own product line.

7. Has your company been part of any legal proceedings (actual suits by or against your company) either currently or in the past? If so, please briefly describe them.

Yes, a patent dispute, settled out of court. November 2013

8. Please provide indication as to whether your firm has been or is the subject of a bankruptcy or insolvency proceeding or subject of assignment for benefit of creditors.

We have not.

9. Who are your five largest customers? Please state the % of your revenue derived from your top 5 customers. Please list the % for each of your top 5 customers separately. (e.g., customer 1 - X%, customer 2 - Y%, customer 5 - Z%).

Customer Name	2015 Revenue from Customer ($)	% of Revenue derived from Customer
Los Angeles Police Department (California)	4,101,102	22.83%
Chicago Police Department (Chicago, IL)	1,665,626	9.27%
Washington State Patrol	940,781	5.24%
New Mexico State Police	646,237	3.60%
Orange County Sheriffs Office (Hillsborough, NC)	475,377	2.65%

2. Service and Quality

10. Identify features and capabilities that differentiate your firm from its competitors.

COBAN is a direct to customer manufacturer that offers a turnkey solution for In car video, Body Worn Cameras, and IP interview room video all managed under ONE centralized Device and Video management software suite. COBAN also offers numerous mass storage solutions including Local, Hybrid, and Cloud. COBAN has been providing mass storage solutions for In car video for over 14 years, longer than any other vendor in the in car / body worn industry. We provide multiple product lines to fit every agency budget, with no "tiered" levels of software. A 5 car PD gets the same functionality and support as a 500 car PD would.

11. What types of Video and Vehicle Equipment does your company specialize in?

COBAN provides digital SD and HD in car video systems, Body Worn Cameras, and IP Interview Room solutions.

12. How much visibility will this contract have at your company in terms of a specific management level?

Due to the wide breadth of products are we are able to offer through this contract platform, this contract will receive a high level of visibility and use from not only the management level, but also our Inside / Outside Sales teams.

3. Product, Breadth & Scope

13. Please explain how you would manage the business for the participating States and multiple sub-political categories, or a geographic regions. If applicable, please provide examples of how you have done this previously for large government or private sector accounts.

Over the past 14+ years COBAN has managed multiple contracts such as this for purchases from various state, county, city and other municipal law enforcement agencies. Each Contract is assigned a contract manager. Each terrirtory is assigned an Inside and Outside sales rep and Field Engineer. Each project is assigned a dedicated Project Manager that works with each agency throughout the entire deployment to ensure the project goes as expected.

14. What are your experiences with providing green products (environmentally friendly) or reduced packaging to current or past clients? Please provide an example.

All of the electronic equipment provided by COBAN is designed to be low power consumption, rechargeable batteries, longer lifespans and have as little impact on the environment as possible.

Oklahoma/NASPO ValuePoint
OK-MA-145 - Public Safety Video and Vehicle Mounted Equipment
Attachment E: Administrative and Technical Proposal Response Template

Administrative Proposal (Mandatory Requirements)

Respondent Name: COBAN Technolgies, Inc.

Instructions:

Fill out the yellow shaded areas only. Blank cells will be considered as "No Response."

Please indicate below your ability to meet the requirements as stated in section 4.1. "Administrative and Technical Response" in the RFP text document. If an item is left blank, you will be implying that your company **cannot** meet the requirement, and your proposal may be eliminated from evaluation. This form must be completed and returned with your response. If additional space is needed to clarify comments, please reference this attachment.

RFP Ref. #	Mandatory Administrative Requirements	Yes/No	Please provide detailed response supporting your answer
4.1.1.	NASPO ValuePoint Statement of Compliance	Yes	COBAN has read and agrees to the NASPO ValuePoint Statement of Compliance.
4.1.2	Insurance	Yes	COBAN's current Insurance plan/carrier already complies with this requirement.
4.1.3.	NASPO ValuePoint Administrative Fee/Reporting	Yes	The reporting contact will be Jeff Lee.
4.1.4	NASPO ValuePoint eMarket Center	Yes	via Hosted Catalog
4.1.5	Lead State Terms and Conditions	Yes	COBAN has read and understands the Lead State Terms and Conditions and the NASPO ValuePoint Master Agreement Terms and Conditions.
4.1.6	References	Yes	Please see included References.
4.1.7	Participating States Terms and Conditions	Yes	COBAN understands that we may be required to negotiate additonal participating state terms and conditions when executing a participating addendum.
4.1.8	Quality Assurance/Warrantee Guarantee	Yes	Please see included Warranty statements for more information.
4.1.9	Product Availability	Yes	COBAN will not cancel any products without an equal and acceptable replacement approved by the Contracting Officer. As a standard practice, if a prouct is reaching End of Life or will no longer be offered, COBAN will give ample notice to all parties involved/affected, and will offer a replacement of equal or greater capabilities.
4.1.10	Emergency Substitutions/Out of Stock	Yes	The requirements set forth by line 4.1.10 in the RFP document are in accordance to COBAN's existing policies.
4.1.11	Account Manager	Yes	Larry Marr, please see included Key Personnel Resumes for information.
4.1.12	Authorized Distributors	No	We do no use distributors to provide product.

4.1.13	Proposed Pricing	Yes	COBAN agrees to the requirements set forth by line 4.1.13 in the RFP document. All potential increases in pricing will be made in writing to the Contracting Officer a minimum 30 days prior to request initiation, and COBAN will provide documentation for justification.
4.1.14	Time of Order	Yes	COBAN will only charge the price agreed upon when an order is placed.
4.1.15	Additional Charges	Yes	COBAN agrees to and complies with the conditions set forth regarding additional charges.
4.1.16	Rebates and Special Offers	Yes	
4.1.17	Disaster Recovery	Yes	Please see included Business Continuity Plan
4.1.18	Professional/Technical Insurance	Yes	COBAN's current Insurance plan/carrier already complies with this requirement. Please see the attached Proof of Insurance document for more info.

Oklahoma/NASPO ValuePoint
OK-MA-145 - Public Safety Video and Vehicle Mounted Equipment
Attachment E: Administrative and Technical Proposal Response Template

Administrative Proposal (Desirable and Scorable Expectations)
Respondent Name: Coban Technologies, Inc.

Instructions:
Fill out the yellow shaded areas only. Blank cells will be considered as "No Response."

Please indicate in the table below your ability to meet the Desirable Administrative Requirements as described in Section 4.2. Please ensure that for each expectation, you are able to meet all the requirements, as outlined in the RFP. If there is a desirable expectation that you are unable to comply with, please propose your company's alternate solution. If an item is left blank, you will be implying that your company **cannot** meet the requirement.

RFP Ref. #	Desirable Service Level Expectations	Yes/No (Can/Cannot meet the expectation)	If YES, describe in detail how you will meet the expectation. If NO, propose an alternative.
4.2.1	Response Time	Yes	Standard response time is within 8 hours during normal business hours.
4.2.2	Delivery Standards	Yes	Typical lead time is 45 days ARO.
4.2.3	Shipping	Yes	All shipments come with packing lists of components shipped as well as serial numbers.
4.2.4	Freight Policy	Yes	All shipments are F.O.B. destination.
4.2.5.	Invoice Accuracy	Yes	invoices are cross referenced against purchase orders and shipping documentation.
4.2.6.	Fill Rate	Yes	Agreed but this number will be different for each agency.
4.2.7.	Ordering Methods	Yes	COBAN agrees to and complies with the stated ordering methods.
4.2.8.	Payment Options	Yes	COBAN agrees to and complies with the stated payment options.
4.2.9.	Invoice Requirements	Yes	COBAN agrees to and complies with the stated invoice requirements.
4.2.10.	Return of Product	Yes	COBAN agrees to and complies with the stated return of product conditions.
4.2.11.	Returns due to User Error	Yes	COBAN agrees to the stated returns due to user error conditions.
4.2.12	Customer Service	Yes	Support hours are from 8:00am - 6:00pm CST Monday - Friday. Please see warranty / maintenance statement for Tech Support problem resolution.
4.2.13	Customer Satisfaction Plan	Yes	Twice a year, COBAN conducts a customer satisfaction survey. Based on customer feedback, Coban will take the appropriate actions to address the customer's concerns.
4.2.14	Past Performance References	Yes	Completed Past Performance References are included in the RFP response.

Oklahoma/NASPO ValuePoint
OK-MA-145 - Public Safety Video and Vehicle Mounted Equipment
Attachment E: Administrative and Technical Proposal Response Template

Technical Proposal (Mandatory and Scorable Requirements)

Respondent Name: Coban Technologies, Inc.

Instructions:

Fill out the yellow shaded areas only. Blank cells will be considered as "No Response."

Please indicate below your ability to meet the requirements as stated in Section 8, Attachment B," Scope of Work" in the RFP text document. If an item is left blank, you will be implying that your company **cannot** meet the requirement, and your proposal may be eliminated from evaluation.

RFP Ref. #	Mandatory Technical Requirements	Agree (Yes / No)	Please provide detailed response supporting your answer
	Attachment D - Band 1		
8.4.2.1.	All body connectors must have safety disengagement features	Yes	External clip on cameras do not "lock" in place, in the event of a struggle, if pulled upon, they will release from the base unit.
8.4.2.2	Log: all recordings, deletions, edits.	Yes	All interactions with recorded videos, users and actions are tracked within the system and a chain of custody log is generated for each file and user for the life of said file / user.
8.4.2.3	Unauthorized deletion or alteration	Yes	Access rights and permissions are configured by the departments administrator based on the various roles that exist in the agency. These access rights determine who has access to the video files and what they can do with them.
8.4.2.4	Predetermined retention period	Yes	Retention periods are defined per event type by the department and their SOP. Once configured, the video management software manages these files based on the retention criteria put in place by the administrator.
8.4.2.5	Retention after investigation has been concluded.	Yes	Retention periods are defined per event type by the department and their SOP. Once configured, the video management software manages these files based on the retention criteria put in place by the administrator.
8.4.2.6	Index and search processes	Yes	There are over 25 different search criteria that can be used to retrieve a video file.
8.4.2.7	Unauthorized Access	Yes	Access rights and permissions are configured by the departments administrator based on the various roles that exist in the agency. These access rights determine who has access to the video files and what they can do with them.
Amend 2	Do you provide instruction manuals at no extra cost?	Yes	Copies of the user manuals will be provided on CD or other type of media.
Amend 2	Do you provide installation manuals at no extra cost?	Yes	Copies of the user manuals will be provided on CD or other type of media.
Amend 2	Do you provide training options?	Yes	Train the Trainer, separate classroom or web based.
Amend 2	Do you have additional warranties which go beyond the normal market standard?	Yes	Please see included warranty / maintenance agreement documents.
	Attachment D - Band 2		
8.5.3.1	Normal Operation Interference	Yes	COBAN's products do not interfere with normal operation of an emergency vehilce. Vehicle safety components are not replaced or removed, and the systems do not cause interference with other electionic systems in operation.
8.5.3.2	Low Battery Indicator	Yes	For both on the unit and wireless mic transmitter.
8.5.3.3	Complete Mountable Solution for different Vehicles	Yes	Mounts available for all standard law enforcement vehicle types.
8.5.3.4	Non Glare Touch or Controlled Video Screen	Yes	5.7" Edge / 4.3" Fusion
8.5.3.5	Record in Non-Proprietary Video Format	Yes	All of COBAN's digital video capture products record in non-proprietary, commercially recognized video formats.

8.5.3.6	Record for both Audio and Video- Inside and Outside Vehicle	Yes	Wireless body mic and in car mic included
8.5.3.7	Wireless Upload Capabilities	Yes	Wireless Upload is a standard feature for the EDGE line of In-Car Video Systems. It is an available, optional module for the FUSION HD. All products feature interrupted upload resume capabilities.
8.5.3.8	Security for Unauthorized Access	Yes	Usage of the In-Car Video systems requires an agency defined ID and password to operate. Removable drives are locked in place and require a key to remove.
8.5.3.9	User Input	Yes	Via touchscreen or Mobile Data Terminal/Laptop integration
8.5.3.10	Authenticate Original File	Yes	Video files have an 128-bit MD5 digital signature created for each one at the time of recording.
Amend 2	Do you provide instruction manuals at no extra cost?	Yes	Copies of the user manuals will be provided on CD or other type of media.
Amend 2	Do you provide installation manuals at no extra cost?	Yes	Copies of the user manuals will be provided on CD or other type of media.
Amend 2	Do you provide training options?	Yes	Train the Trainer, separate classroom or web based.
Amend 2	Do you have additional warranties which go beyond the normal market standard?	Yes	Please see included warranty / maintenance agreement.
	Attachment D - Band 3		
8.6.1.1	CJIS Security Addedum	Yes	COBAN agrees to sign the CJIS Security Addendum with each requesting Agency.
8.6.1.2	Personnel , CJIS Background, Fingerprint	Yes	Microsoft Azure Government, the SaaS Cloud provider that COBAN uses, complies with CJIS requirements, including background checks and fingerprint registration. Please see attached Azure Government Overview document or visit https://www.microsoft.com/en-us/TrustCenter/Compliance/CJIS for details.
8.6.1.3	Security Audits	Yes	All interactions with recorded videos, users and actions are tracked within the system and a chain of custody log is generated for each file and user for the life of said file / user.
8.6.1.4	Understands CJIS Security Policy	Yes	COBAN has read and understands the CJIS Security Policy.
8.6.1.5	Separate, isolated cloud platform	Yes	Please refer to the attached Azure Government Overview document.
8.6.1.6	Certification State(s) retain ownership of data	Yes	All data and video ownership will remain with the respective state/agency throughout the contract and project. COBAN does not take ownership at any point.
8.6.1.7	All data kept within continental United States	Yes	Cloud service servers are located in the continental United States only. Local storage servers will be located on premise of the respective state/agency.
8.6.1.8	Chain of custody	Yes	All interactions with recorded videos, users and actions are tracked within the system and a chain of custody log is generated for each file and user for the life of said file / user.
8.6.1.9	All contracted work inside United States	Yes	If COBAN were to use contracted work for a specific project, it will be inside the United States.
8.6.1.10	Video sharing	Yes	Sharing with video evidence with groups inside and outside of an Agency are possible with all storage solutions provided by COBAN.
8.6.1.11	Controlled access to evidence	Yes	Access rights and permissions are configured by the department's local system administrator based on the various roles that exist in the agency. These access rights determine who has access to the video files and what they can do with them.
8.6.1.12	Multiple indexes, files, tags without altering original video	Yes	There are over 25 different search criteria that can be used to retrieve a video file.

8.6.1.13	Redaction system	Yes	The COBAN solution records videos in commerically recognized formats, and is compatible with several third party Redaction programs. Native redaction capabilities will be available in 2017.
Amend 2	Do you provide instruction manuals at no extra cost?	Yes	Copies of the user manuals will be provided on CD or other type of media.
Amend 2	Do you provide installation manuals at no extra cost?	Yes	Copies of the user manuals will be provided on CD or other type of media.
Amend 2	Do you provide training options?	Yes	Train the Trainer, separate classroom, or web based.
Amend 2	Do you have additional warranties which go beyond the normal market standard?	Yes	Please see included warranty / maintenance agreement.
	Attachment D - Band 4		
8.7.1.a	Breadth of product coverage. Multiple makes and models of vehicles?	No	COBAN will not be bidding on Band 4 items.
8.7.1.b	Products made for Law Enforcement?	No	COBAN will not be bidding on Band 4 items.
8.7.1.c	Seat Belts latch or attach by exterior door?	No	COBAN will not be bidding on Band 4 items.
8.7.1.d	Partition Materials?	No	COBAN will not be bidding on Band 4 items.
8.7.1.e	Vehicle Console Options?	No	COBAN will not be bidding on Band 4 items.
Amend 2	Do you provide instruction manuals at no extra cost?	No	COBAN will not be bidding on Band 4 items.
Amend 2	Do you provide installation manuals at no extra cost?	No	COBAN will not be bidding on Band 4 items.
Amend 2	Do you provide training options?	No	COBAN will not be bidding on Band 4 items.
Amend 2	Do you have additional warranties which go beyond the normal market standard?	No	COBAN will not be bidding on Band 4 items.

11375 West Sam Houston Parkway South # 800
Houston, Texas 77031

SECTION 4

Offeror Narrative

- COBAN EDGE SD Solution Overview
- COBAN EDGE Hi-Def Solution Overview
- COBAN FUSION HD Solution Overview
- COBAN ECHO Solution Overview

Product Brochures

- COBAN EDGE SD In-Car Video
- COBAN EDGE Hi-Def In-Car Video
- COBAN FUSION HD In-Car Video
- COBAN ECHO Body Worn Camera
- COBAN Digital Video Management System
- COBAN Command Center
- Digital Property Manager

ECHO Body Worn Camera

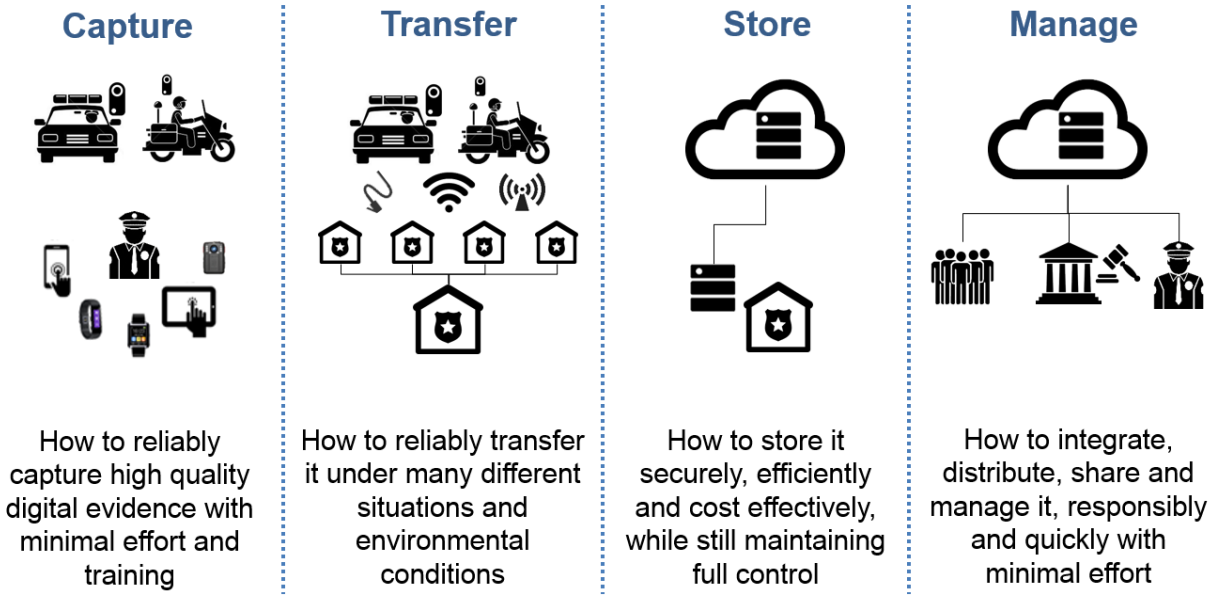
11375 West Sam Houston Parkway South # 800
Houston, Texas 77031

Introduction

The COBAN ECHO, in conjunction with the COBAN Digital Video Management System (DVMS), provides a powerful and varied function set intended for use by law enforcement and public safety industries. The ECHO is modular in design, both in terms of configuration and scale. The following information explains the major functions of our solution and how they will meet your requirements.

COBAN Solutions Overview

There are four phases to BWC digital video projects that form the life cycle of video evidence. This document will describe the flexibility, security, and scalability of COBAN's solutions in regards to these aspects:



Video Capture

COBAN's video capture solutions offer utility that can be scaled and configured to fit the needs of any law enforcement agency. The focus of this overview will be the COBAN ECHO and its related components.

COBAN Body Worn Camera

COBAN's ECHO is designed as a high performance body worn video recorder with the understanding that technology requires both usability and capability. The ECHO possesses features that are intuitive for the user and is centrally managed from the back office COBAN Digital Video Management System.

Simple Operation

The ECHO has an intuitive button layout that is devised for ease-of-use while still being customizable from the back office management software. For example, if the agency policy requires fast activation, a single button press can initiate recording. But if policy dictates that recording should be slightly delayed to prevent accidental recordings, activation can be configured to be a double-click or 3-second button press. Either of the top buttons located on the sides of the unit can be programmed to start recording, making operation with either hand possible. There are no switches or multiple inputs for the user to worry about during operation.

Adjustable Video Resolution

The ECHO has the ability for local system administrator-defined video resolution and bit rates. Depending upon the department's policy, the DVMS administrator can set the ECHO to record anywhere from standard definition to true 1080p high definition. The agency can balance what they decide is acceptable video quality between battery life and data storage considerations.

Recording Quality

The recording quality of the ECHO is optimized for high image quality in different environmental conditions. Even during movement or vibration, the image does not heavily pixelate or lose focus. The ECHO features a fixed lens optimized for focus and stability, auto-white balance, and brightness control.

Programmable Invisible IR Illuminator

For nighttime or lowlight operation, the ECHO provides a built-in IR light source that may be configured according to policy. If IR light is enabled, it will automatically turn on and off based on ambient light sensors. If it is disabled, the ECHO will provide an image that closely emulates what the human eye perceives.

Covert Function

The ECHO also has a covert mode that disables all visual indicators. If needed, any audio indicators may also be turned off, allowing for silent operation. These options are once again controlled centrally by the local system administrator, ensuring standardized settings and operation for groups or even across all users.

Integrated with COBAN EDGE Hi-Def

The ECHO can connect to the EDGE Hi-Def In-Car Camera system via a single bay docking station. Videos and data from the ECHO can then be transferred to the EDGE Hi-Def for purposes of data entry, video review, or simultaneous upload with the In-Car video. If the videos from both the Body Worn Camera and In-Car Camera system are uploaded together, they can be automatically linked together as a single case event when managed from the back office.

Event Data Collection

Data helps to identify and organize captured video.

Event data such as type of offense, offender's information, case numbers, and more can be entered using the In-Car Camera System, Mobile Data Terminal (laptop), or COBAN DVMS software. This data can be used to attain a more complete understanding of the incident in question, and sort the uploaded videos for easier organization down the line.

These are just a few of the customizable functions available for all ECHO deployments. Many BWCs can offer some basic level of compliance, especially when it comes to capturing video, but the COBAN ECHO is set apart due to flexibility that allows it to adapt to any situation.

Video Transfer

COBAN's video transfer solutions are designed to ensure efficient turnkey application. The transfer process, as the link between front-end and back-end, is essential in determining the flow and efficacy of a solution.

If ECHO is the department's only COBAN product, transferring data is as simple as docking the unit into an upload/charging bay. The files will automatically begin transferring to the workstation at a

rate for 24.6 GB per hour. As an example, four hours of 720p video will be able upload in less than ten minutes. Single and six port upload/charging bays are available to accommodate the department's necessities. All this is accomplished automatically while the ECHO is charging in a bay, so there is no need to allocate additional time or manpower to the process. If a bay is not available, the ECHO can be connected to the computer by secure USB.

ECHO Transfer Process Diagram

If the ECHO is integrated with a COBAN EDGE Hi-Def system, the user can transfer recorded data directly to the in-car unit. The videos and data from both BWC and in-car sources can then be uploaded together, either through wireless upload or direct transfer via the physical data infrastructure.

If the department uses Mobile laptops, the ECHO can also be connected through USB or the single upload/charging bay in the car. Once connected to the MDC, the user can review recordings, tag, and enter metadata that will be transferred with the video once it is uploaded at the station.

Video Storage

COBAN offers several types of video storage to accommodate the specific needs of a department, no matter how small or large. In instances where a storage network is already in place, COBAN can work with the agency to ensure compatibility and sustainability. Types of storage we offer include Local Primary Storage, Extended Storage, Cloud storage, and Hybrid solution. The following information details each of these different forms.

Local Primary Storage

Local Primary Storage is when videos are hosted on a nearby server with internal storage or an attached disk array. The videos are available for viewing to whoever possesses the access rights. Local Primary Storage is used when the videos in question have been recently uploaded or will be accessed frequently. Local Primary Storage provides the fastest transfer rates of all the storage options and immediate access to all data located on the server or disk array. At this stage, the department can still maintain complete control over security and ownership of their data.

COBAN can recommend a disk storage system that fits within the department's projected requirements and budget, while maintaining flexibility for future growth. Points to consider when making this recommendation include the amount of video generated on a daily basis and the length of time that videos need to be quickly retrieved on line.

Typically, Local Primary Storage incurs higher initial costs when compared to Cloud or remote storage. However, there are no further usage or access fees after the initial deployment. So for departments with heavy network usage, over longer periods of time, local storage will be the more cost effective choice.

Local Extended Storage

Local Extended Storage is used to retain videos and data for longer durations than Local Primary Storage. This can be anywhere from a few months to years past the departments online requirement. Videos that are not accessed often or marked as critical will be moved from Primary over to Extended Storage for retention purposes. Local Extended Storage may take the form of a secondary server, Network-Attached Storage, Direct-Attached Storage, Storage Area Network, or even DVDs. COBAN's solution provides the flexibility to initiate the required network infrastructure (a server) or expand the department's existing long-term data storage.

COBAN's Auto DVD Solution is an extended storage option that does not require additional IT personnel to operate. It provides a local, on-site solution that incorporates well with any preexisting infrastructure. With Auto DVD Solution, any video matching preconfigured event types are automatically sent to the DVD robot for export. After a DVD is written, it can be retained locally or given to the proper official for courtroom purposes. Anywhere from one to five copies per video can be exported depending upon the department's standard operating procedure. The Auto DVD Solution is designed to eliminate the man hours spent exporting and creating DVDs manually.

Cloud Storage

Cloud Storage is a remote based solution. It involves uploading all captured video and data directly to a remote server where it will be hosted by another party. There is no designation between online and archived data, and if access is required, a video will need to be downloaded from the Cloud server. The appeal of Cloud Storage is that it lessens the need for IT personnel and investment in storage hardware, since there is no need for intermediary local servers. The Cloud is a viable solution for departments that possess robust network bandwidth.

COBAN utilizes industry-leading Microsoft Azure Government for Cloud storage services. Microsoft Azure Government is CJIS capable, FedRAMP compliant, and DISA certified to ensure the security of data. Cloud services do not require separate licenses or access administration and data management are still done within the Digital Video Management system.

While the initial cost of Cloud is much lower than that of local storage, subscription fees and increasing data volume eventually lead to higher than anticipated expenditures. Also, since the Cloud is so heavily dependent on bandwidth, not all agencies will be equipped to realistically implement this type of storage system. It is not a universal solution and COBAN will cooperate with the department to make sure there is a clear understanding of the potential benefits provided by the Cloud.

Hybrid Storage Solution

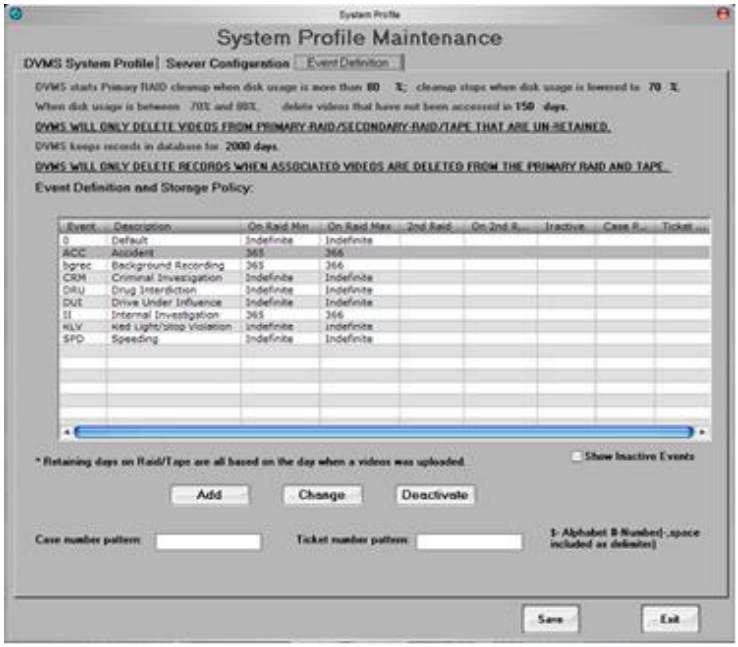
The Hybrid Storage Solution is a partial combination of the concepts behind Local and Cloud storage systems. Rather than immediately pushing all data to the Cloud, videos are initially uploaded to a caching device. Certain or all types of videos, in accordance to department policy, can be kept locally for easier and more immediate retrieval. The videos are then scheduled for automatic upload to the cloud for retention purposes. The time frame for pushing videos to the Cloud can be configured by the local system administrator. For example, if network bandwidth is a concern and the cloud is used solely for long term storage purposes, videos can be uploaded at off-peak hours.

The strength of the hybrid solution is that it can conform to the existing infrastructure to ensure impact on the network is minimized. It is not necessary to acquire multiple servers at one location or augment internet access capabilities. Along these lines, the Hybrid solution decreases the strain on bandwidth when compared to a Cloud solution, as uploads can be arranged to occur at off-peak times instead of all at once, and a copy of high priority event type videos can be kept on the caching device to avoid having to re-download the file for access. The Hybrid solution may not be compatible with a department's needs because it still requires some local infrastructure and IT personnel, while the fees associated with Cloud storage are still applicable, albeit at a lower tier. But for certain departments, dependent upon size and usage, a Hybrid solution has the potential to fit storage requirements while minimizing the necessary investment in new infrastructure.

The storage solution provided by COBAN will always comply with each individual agency's capabilities and requirements. Our aim is to provide a functional and complete solution that will not conflict with the department's budget or capabilities.

Video Management

COBAN's Digital Video Management System is a back office, policy-based automation software that allows administrators to focus on overall system performance instead of day-to-day operational tasks.



Video Retention

The systems administrator determines how each category of video is handled; retention period for each video is connected to its type. Once the retention period has passed and no deliberate action has been taken, videos are purged from the system automatically. This guarantees policy compliance while minimizing the amount of time spent micromanaging files.

Automated System Management

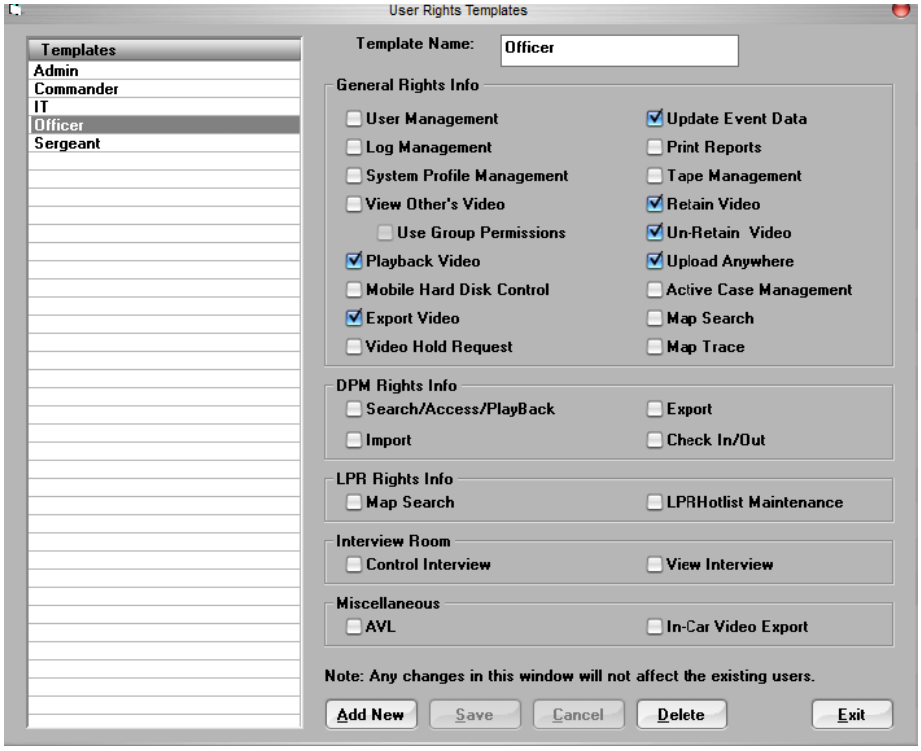
After the administrator defines the necessary criteria, DVMS will take over the everyday video management jobs. Diagnostic reports will be generated, showing the results of daily tasks and overall storage status. System exceptions are also emailed to alert the system administrator for immediate review.

Complete Chain of Custody

All activities associated with each uploaded video are logged to the system's audit trail. This includes the date and time a video was uploaded, archived, played back, exported, or purged from the system. A complete history of each video is available to the system administrator for analysis.

System Security

Activity permissions such as video access, report printing, and general data management functions can be set up by the administrator. Only users with proper clearance are able to perform actions associated with a video in question, and all activities are logged into the aforementioned audit trail.



Centralized Management System

DVMS is capable of managing videos and data from both COBAN Body Worn Cameras and In-Car Video systems. Organization and management of videos involves the same interface and procedures regardless of the source. In addition, associated videos can be grouped together into a case file for easier organization.

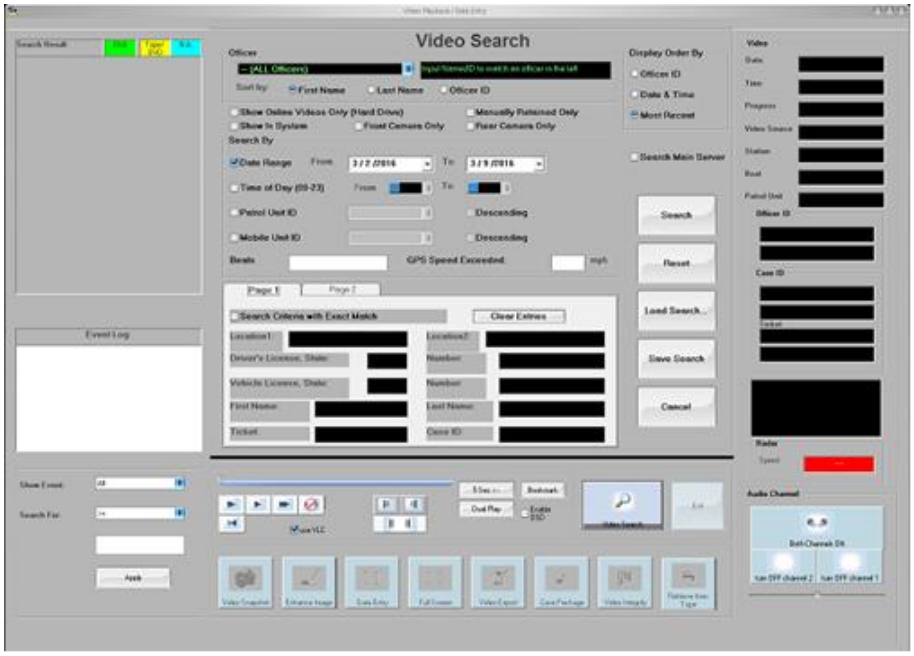
Streamlined Storage Management

Whether the department uses Local, Cloud, or Hybrid storage, DVMS provides a standard management system that does not require changes to user interface or external software. Storage server policy, once established by the local system administrator, is automated while still allowing specific videos and data to be handled on an individual basis.

Powerful Search Capability

Videos can be searched using all event data associated with the BWC units, including offender's ID, patrol unit, event type, time range, and more. The multiple criteria selection allows the user to find

specific videos or perform general inquiries. The following graphic shows an example of the interface and options of the DVMS search function.



COBAN Courier

COBAN Courier service allows the department to export videos or Digital Property Management case files without the need for physical DVDs. When the department uploads the requested video, a link will be sent via email to the intended recipient so he or she may access/download it. The link is time-sensitive and the duration can be configured as necessary. Although Courier service is Cloud based, it does not require a COBAN Cloud subscription to be available for use.

Digital Property Manager (DPM)

DPM is value added software that is included within DVMS. It imports, aggregates, and manages externally sourced digital evidence like videos, audio, or documents based on case number.

Users can add external files into the system or link to in-car and interview room videos to form a case package. The system maintains all versions of each individual file in addition to an audit trail to track activity. There is also an export function that allows the user to send all the digital evidence to a DVD, with a searchable index for easy reference.

Distributable Video Playback Tool

When videos are transferred to DVD or other portable media, DVMS can include an installation program for playback viewing. The program will install a video playback tool on any Windows XP, Vista, 7, or 10 based computers. All the event data present will be displayed along with the video, giving a more complete depiction of what is happening on-screen. Although Windows Media Player or VLC Player are capable of showing the videos, the program provided by COBAN provides an interface identical to the DVMS software.

Data Replication

Data redundancy is important for every agency in order to guarantee necessary videos and data will not be lost due to server or storage failure. COBAN provides departments the flexibility to decide how they copy videos and data to a secondary source. Local storage, DVDs, Cloud, or even a hybrid solution are all compatible with the COBAN system. Agencies also have the choice to replicate just videos, event based data, or all data according to their policies.

COBAN Enterprise Solution is specifically designed for multiple precinct agencies and provides several functions.

1. All data under department domain, including officers, vehicles, and event definitions, can be centrally maintained. A main server acts as a single data maintenance point, and updated data will be pushed to all sub-stations on a daily basis, allowing for consistent data content across all sites.

2. Event data is accumulated at the main server, which then enables query and playback of videos amongst the sub-stations across the network.

3. After program updates for both in-car and backend software are loaded onto the main server, sub-stations will receive the updates automatically.

All of the aforementioned functions do not need to be enabled. Departments can choose which features are most suited for department policy. As an example, if network bandwidth is a concern, videos can be stored at the sub-stations while event data is pushed to the main server. In this instance, even though COBAN is providing distributed storage architecture, an approved user can access any video on the network for the purposes of viewing or exporting. The Enterprise Solution furthers the flexibility, interconnectivity, and network capabilities inherent in COBAN's end-to-end system.

COBAN Solution Overview

EDGE SD

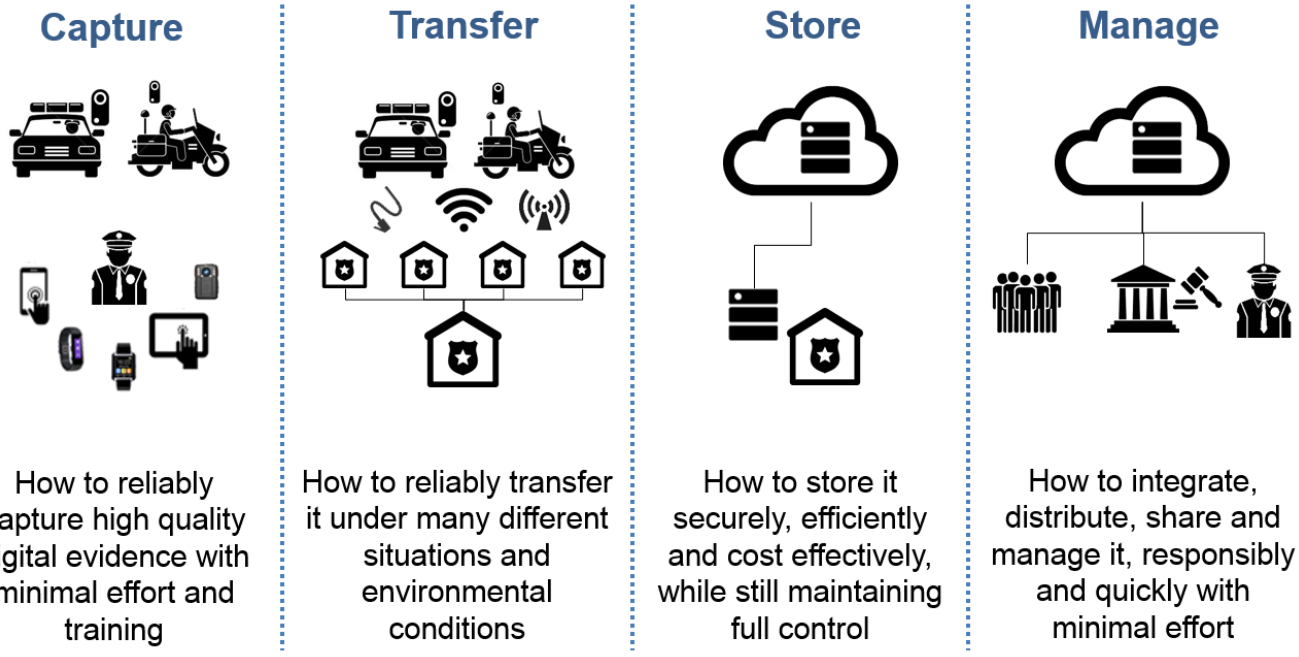
11375 West Sam Houston Parkway South # 800
Houston, Texas 77031

Introduction

The solution proposed by COBAN offers a powerful and varied function set intended for use by law enforcement and public safety industries. The products and services provided by COBAN are modular in design, both in terms of configuration and scale. The following information explains the major functions of our solution and how they will meet your requirements.

COBAN Solutions Overview

There are four phases to digital video projects that form the life cycle of video evidence. This document will describe the flexibility, security, and scalability of COBAN's solutions in regards to these aspects:



Video Capture

COBAN's video capture solutions offer utility that can be scaled and configured to fit the needs of any law enforcement agency. The focus of this overview will be the COBAN EDGE SD and its related components.

COBAN EDGE SD

COBAN's EDGE SD systems are designed as high performance mobile digital video recorders with the understanding that technology requires both usability and capability. EDGE SD possesses features that are not only intuitive for the user, but easily incorporate into the agency's data management ecosystem. COBAN will also provide mobile laptop integration software, allowing the officer to control the EDGE SD system via his or her in-car computer. The proceeding information highlights the capabilities of the EDGE SD.

Multiple-Camera Support

Cameras are the basis for digital video recording. It may seem obvious, but the number and position of cameras are important factors in determining the effectiveness of a system.

The EDGE SD is capable of supporting up to 6 cameras and several different configurations depending on the department's needs. The local administrator can adjust how the cameras operate by using the back office software provided by COBAN.

Dual-Wireless Microphone

Sound is a significant aspect of any officer related incident. In conjunction with visual evidence, audio recordings give insight to the situation at hand.

EDGE SD supports two wireless transmitters plus a covert in-car microphone. All three microphones can be controlled separately. The wireless transmitters also have two programmable buttons in addition to the record button. Functions that can be mapped to these buttons include mute, bookmark, camera auto-zoom, stop recording, partner alert, or covert recording.

The partner alert function is used to trigger the partner's transmitter to vibrate and/or light up, dependent upon the back office configuration. If the transmitters are set to covert mode, there will be no response so as to not compromise the officer's position.

The covert recording function allows the officer to remotely begin a rear seat camera recording while blanking out the system's monitor. When suspects are placed in the back seat, they will have no indication that they are being recorded.

Flexible Pre-Event and Post-Event Recording

Pre-event and post-event recording is important in guaranteeing the entirety of an event is captured on video.

The local administrator can configure the desired length of pre- and post-event recording without restrictions. If needed and allowed by policy, the officer may adjust the buffer size while in the car.

Fail-Safe Recording

Fail-safe recording ensures that captured video is retained in case of accidents or localized failure. This is achieved by duplicating all video content to both the CPU's internal drive and the removable hard drive. If for some reason a drive experiences failure, there will always be a backup copy on the other. With this feature, it is less likely that important video is lost due to unforeseen circumstances.

Smart Power Monitoring

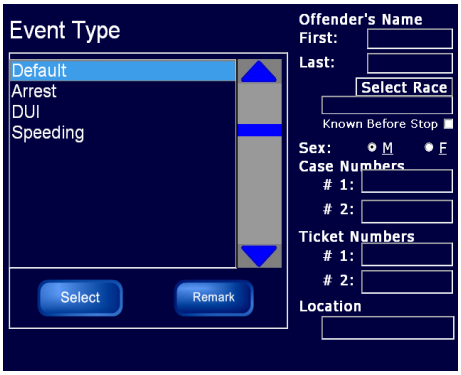
Every in-car system offered by COBAN comes with Smart Power Monitoring as a standard function. The hardware module that controls this feature is built into the main CPU unit, so there are no external components beyond a small, replaceable UPS battery.

Smart Power Monitoring controls the power transmitted to a system, protecting against damage to both the unit and the car itself. For example, if the voltage provided by the car is insufficient, the system will alert the officer, switch to the backup UPS source, and begin a delayed shutdown process. This prevents the in-car system from draining the car battery and causing software corruption due to improper shutdown.

Smart Power Monitoring also creates a log file that constantly tracks the power readings, system actions, and triggers activated during a shift. The log will be updated from the moment a unit is powered on to the point the system is powered off. This is a useful diagnostic tool in case there are any hardware issues, as it allows insight to the operational environment.

In addition, if there are any possible problems detected, the system can send out an automatic email to notify the proper personnel that maintenance may be required.

Event Data Collection



Event data helps to identify captured video and provides additional incident information.

Data such as the type of offense, offender's information, case numbers, and more can be entered using a keyboard, the touch screen monitor, or magnetic strip reader. This data can be used to attain a more complete understanding of the incident in question, and sort the uploaded videos for easier organization down the line.

Metadata Collection

Metadata provides additional data that may prove helpful in identifying when, where, and how an incident occurred.

Information such as date/time, light bar status, speed radar readings, and GPS coordinates can be recorded automatically through various digital trigger connections. Like event data, this can lead to a more complete understanding of the circumstances surrounding an incident.

Configurable Triggers

Input triggers allow a certain amount of automation once a specific action is initiated. For example, when a patrol car's light bar is activated, triggers may also initiate recording. These are set by the administrator through DVMS, and are included in the metadata associated with a recording.

Snapshot Function

Officers have the capability to capture snapshots using the system's front camera. These snapshots can then be reviewed in the car, exported along with videos, or uploaded separately to servers.

Bookmark Function

Officers can insert "bookmarks" into captured videos during recording or in-car playback. Bookmarks serve as metadata tags after videos are uploaded to the server. When a video is reviewed at a workstation, these bookmarks can be used to jump to a corresponding time point, indicating an important occurrence.

GPS and Mapping Software

GPS is offered as a standard accessory for EDGE SD systems. COBAN's Digital Video Management Software can use GPS data to highlight a patrol car's physical location, overlaid on a regional map. The mapping function can also be used to initiate video streaming once a patrol car is in specific range. A proper wireless infrastructure must be in place for streaming to happen.

Automated In-Car System Update

In some cases, it may be necessary for administrators to update or modify the user settings of the in-car systems. This can be an overwhelming task if done on an individual unit basis.

COBAN's solution allows for an easy update process. Any settings defined by the system administrator can be transmitted to any in-car unit at the end of a wireless upload or through the process of checking out a removable hard drive.

ECHO Body Worn Camera Integration

The EDGE SD can be integrated with the COBAN ECHO Body-Worn Camera solution. Users can transfer recorded data directly from the Body-Worn Camera to the in-car unit. The videos and data from both BWC and in-car sources can then be uploaded together, either through wireless or direct transfer via the data infrastructure.

Video Transfer

Video transfer for the EDGE SD involves video upload, video streaming, and inter-precinct transfer. Transfer is a critical step in the lifecycle of digital video evidence; problems sometimes occur at this stage because of bottlenecking or inefficiencies in infrastructure. COBAN's video transfer solutions are designed to lessen the probability of difficulties and ensure availability of all digital video properties.

Video Upload

COBAN's solution provides three upload methods for flexibility and fail-safe protection. Depending upon an agency's protocol and infrastructure, any one or a combination may suit upload requirements.

Wireless Upload

COBAN's wireless upload method uses 802.11 a/g/n/ac protocol for high speed uploading. The wireless network card is built into the main unit; there are no separate modules required to install.

If, for any reason, an upload session does not complete, a checkpoint transfer algorithm allows the upload to be interrupted and resumed at a later time without having to start over from the beginning. Also, when there are time constraints, specific videos can be selected by the officer for priority upload. The remaining videos will be uploaded at the next available opportunity.

The system administrator can designate how the in-car units access the wireless upload server. Settings can be configured to actively search for the upload server and automatically begin the uploading process once a connection is established, or to upload videos only when the officer explicitly instructs the system to do so.

It is sometimes difficult for agencies to anticipate just how much strain on a network is possible when there are numerous uploads occurring all at once. If wireless upload is a practical option, COBAN will provide recommendations for wireless networks and collaborate with departments to address the possible limitations.

Wired Upload

COBAN's wired upload method uses both 100BASE-T and Gigabit Ethernet network interface. Wired upload is much faster than wireless, but requires cabling and physical stations that will connect the car to the network. Wired upload presents its own set of challenges, and COBAN will consult with the agency regarding equipment specifications, durability, network security, and personnel safety.

Removable Media Upload

COBAN also provides removable, industrial grade Solid State Drives as a functional upload solution. These removable hard drives are encased in a hardened shell for extreme durability and can be transported without fear of physically breaking. For security purposes, the hard drive is only accessible by using a specially designed cradle what will connect to any high-speed USB 2.0 or 3.0 interface. This is the fastest and most efficient method of uploading for departments that have tight turnaround shifts.

Removable drives are standard with every COBAN in-car system, and can function as the primary upload system or as a backup method if there are any network issues.

Video Streaming

When an officer initiates event recording, the EDGE SD can stream videos to the backend dispatch or control center. Any IP based wireless network is compatible, and available bandwidth will directly affect how many FPS are transmitted. If the network bandwidth is not capable of supporting video streaming, the department has the option of transferring live snapshots every few seconds. COBAN's DVMS software is able to simultaneously display up to 16 streaming videos or live images on each workstation's display.

Inter-Precinct Transfer

For departments that have multiple precincts, it is important to have any uploaded videos and data available to all approved users across the network without compromising security. To address this, COBAN provides both centralized and distributed video storage. Dependent upon the department's existing infrastructure and budgeted funds, COBAN will work to recommend the best solution that fits current needs without restricting potential growth.

Even if distributed video storage is used, all the metadata can be pushed to the central server with minimum bandwidth requirement. All authorized users on the department network, no matter the physical location, will be able to locate, playback, and export any video stored on the regional servers.

Video Storage

COBAN offers several types of video storage to accommodate the specific needs of a department, no matter how small or large. In instances where a storage network is already in place, COBAN can work with the agency to ensure compatibility and sustainability. Types of storage we offer include Local Primary Storage, Extended Storage, Cloud storage, and Hybrid solution. The following information details each of these different forms.

Local Primary Storage

Local Primary Storage is when videos are hosted on a nearby server with internal storage or an attached disk array. The videos are available for viewing to whoever possesses the access rights. Local Primary Storage is used when the videos in question have been recently uploaded or will be accessed frequently. Local Primary Storage provides the fastest transfer rates of all the storage options and

immediate access to all data located on the server or disk array. At this stage, the department can still maintain complete control over security and ownership of their data.

COBAN can recommend a disk storage system that fits within the department's projected requirements and budget, while maintaining flexibility for future growth. Points to consider when making this recommendation include the amount of video generated on a daily basis and the length of time that videos need to be quickly retrieved on line.

Typically, Local Primary Storage incurs higher initial costs when compared to Cloud or remote storage. However, there are no further usage or access fees after the initial deployment. So for departments with heavy network usage, over longer periods of time, local storage will be the more cost effective choice.

Local Extended Storage

Local Extended Storage is used to retain videos and data for longer durations than Local Primary Storage. This can be anywhere from a few months to years past the department's online requirement. Videos that are not accessed often or marked as critical will be moved from Primary over to Extended Storage for retention purposes. Local Extended Storage may take the form of a secondary server, Network-Attached Storage, Direct-Attached Storage, Storage Area Network, or even DVDs. COBAN's solution provides the flexibility to initiate the required network infrastructure (a server) or expand the department's existing long-term data storage.

COBAN's Auto DVD Solution is an extended storage option that does not require additional IT personnel to operate. It provides a local, on-site solution that incorporates well with any preexisting infrastructure. With Auto DVD Solution, any video matching preconfigured event types are automatically sent to the DVD robot for export. After a DVD is written, it can be retained locally or given to the proper official for courtroom purposes. Anywhere from one to five copies per video can be exported depending upon the department's standard operating procedure. The Auto DVD Solution is designed to eliminate the man hours spent exporting and creating DVDs manually.

Cloud Storage

Cloud Storage is a remote based solution. It involves uploading all captured video and data directly to a remote server where it will be hosted by another party. There is no designation between online and archived data, and if access is required, a video will need to be downloaded from the Cloud server. The appeal of Cloud Storage is that it lessens the need for IT personnel and investment in storage hardware, since there is no need for intermediary local servers. The Cloud is a viable solution for departments that possess robust network bandwidth.

COBAN utilizes industry-leading Microsoft Azure Government for Cloud storage services. Microsoft Azure Government is CJIS capable, FedRAMP compliant, and DISA certified to ensure the security of data. Cloud services do not require separate licenses or access administration and data management are still done within the Digital Video Management system.

While the initial cost of Cloud is much lower than that of local storage, subscription fees and increasing data volume eventually lead to higher than anticipated expenditures. Also, since the Cloud is so heavily dependent on bandwidth, not all agencies will be equipped to realistically implement this type of storage system. It is not a universal solution and COBAN will cooperate with the department to make sure there is a clear understanding of the potential benefits provided by the Cloud.

Hybrid Storage Solution

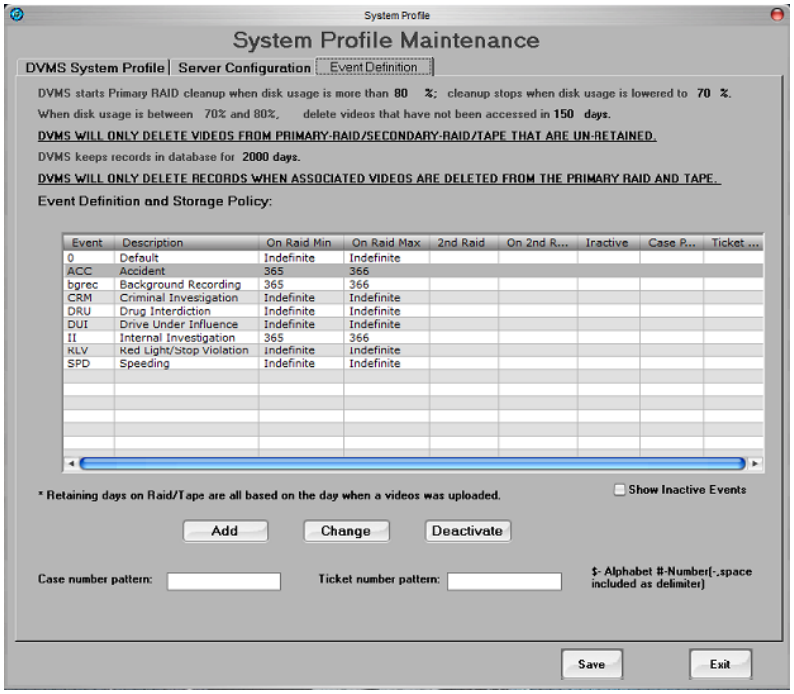
The Hybrid Storage Solution is a partial combination of the concepts behind Local and Cloud storage systems. Rather than immediately pushing all data to the Cloud, videos are initially uploaded to a local gateway. Certain types of videos, in accordance to department policy, can be kept locally for easier and more immediate retrieval. All other types of videos, or videos that have passed a specified time frame with no deliberate action taken, can then be scheduled for automatic upload to the cloud for retention purposes.

The strength of the hybrid solution is that it can conform to the existing infrastructure to ensure impact on the network is minimized. It may not be necessary to acquire multiple servers or augment internet access capabilities. Along these lines, the Hybrid solution decreases the strain on bandwidth when compared to a Cloud solution, as uploads are arranged to occur at off-peak times instead of all at once. The Hybrid solution may not be compatible with a department's needs because it still requires some local infrastructure and IT personnel, while the fees associated with Cloud storage are still applicable, albeit at a lower tier. But for certain departments, dependent upon size and usage, a Hybrid solution has the potential to fit storage requirements while minimizing the necessary investment in new infrastructure.

The storage solution provided by COBAN will always comply with each individual agency's resources and requirements. Our aim is to provide a functional and complete solution that will not conflict with the department's budget or capabilities.

Video Management

COBAN's Digital Video Management System is a back office, policy-based automation software that allows administrators to focus on overall system performance instead of day-to-day operational tasks.



Centralized In-Car Policy Setting

The system admin can set up many in-car options through the backend software, including how units respond to input triggers, the functions of the wireless microphone's programmable buttons, the duration of pre-event and post-event recording, and more. Once it has been determined, the settings will be pushed to the in-car units at the end of an upload session or during the process of removable hard drive checkout. Changes in department policy can be easily implemented for the whole fleet without the need to schedule downtime.

Video Retention

The systems administrator determines how each category of video is handled; retention period for each video is connected to its type. Once the retention period has passed and no deliberate action has been taken, videos are purged from the system automatically. This guarantees policy compliance while minimizing the amount of time spent micromanaging files.

Automated System Management

After the administrator defines the necessary criteria, DVMS will take over the everyday video management jobs. Diagnostic reports will be generated, showing the results of daily tasks and overall storage status. System exceptions are also emailed to alert the system administrator for immediate review.

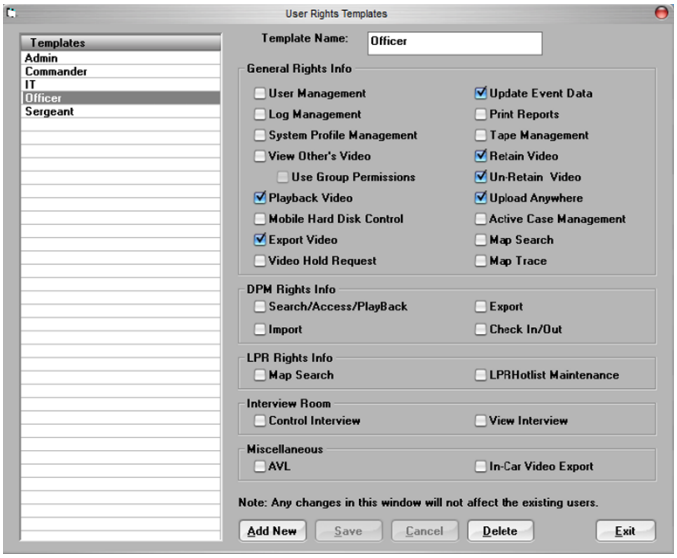
Complete Chain of Custody

At the time of capture, each video is associated with a digital signature that is generated using an MD5 Hash Algorithm, providing integrity verification.

All activities associated with each uploaded video are logged to the system's audit trail. This includes the date and time a video was uploaded, archived, played back, exported, or purged from the system. A complete history of each video is available to the system administrator for analysis.

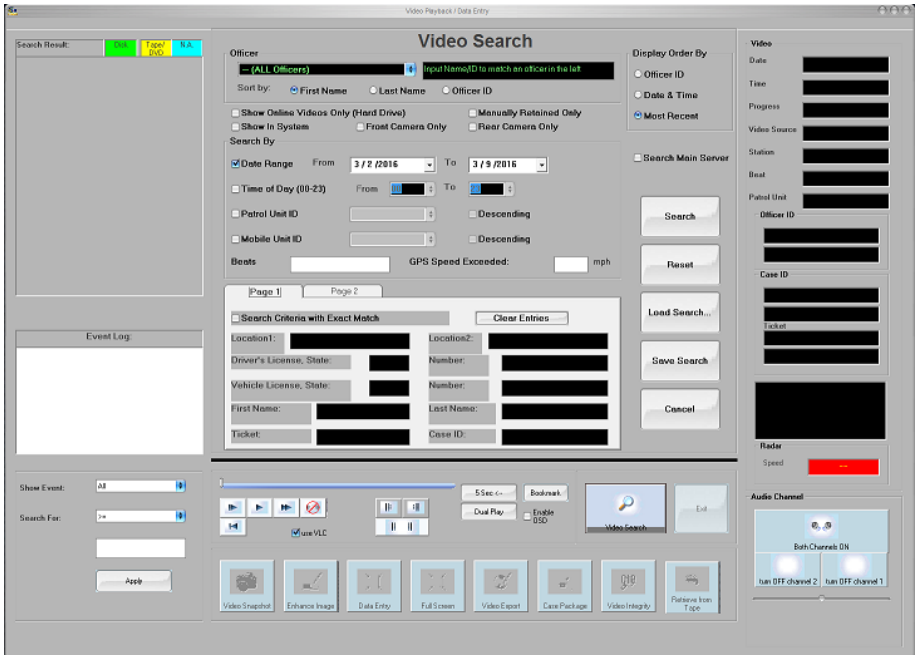
System Security

Activity permissions such as video access, report printing, and general data management functions can be set up by the administrator. Only users with proper clearance are able to perform actions associated with a video in question, and all activities are logged into the aforementioned audit trail.



Powerful Search Capability

Videos can be searched using all event data associated with the in-car units, including offender's ID, patrol unit, event type, time range, and more. The multiple criteria selection allows the user to find specific videos or perform general inquiries.



GPS Support

If GPS is implemented, a map interface may be used to search for videos. Also, there is a Route Trace function in DVMS that allows authorized personnel to view the course a car has taken throughout a shift.

Digital Property Management (DPM)

DPM is value added software that is included within DVMS. It imports, aggregates, and manages externally sourced digital evidence like videos, audio, or documents based on case number.

Users can add external files into the system or link to in-car and interview room videos to form a case package. The system maintains all versions of each individual file in addition to an audit trail to track activity. There is also an export function that allows the user to send all the digital evidence to a DVD, with a searchable index for easy reference.

COBAN Courier

COBAN Courier service allows the department to export videos or Digital Property Management case files without the need for physical DVDs. When the department uploads the requested video, a link will be sent via email to the intended recipient so he or she may access/download it. The link is time-sensitive and the duration can be configured as necessary. Although Courier service is Cloud based, it does not require a COBAN Cloud subscription to be available for use.

Distributable Video Playback Tool

When videos are transferred to DVD or other portable media, DVMS can include an installation program for playback viewing. The program will install a video playback tool on any Windows XP, Vista, 7, or 10

based computers. All the event data present will be displayed along with the video, giving a more complete depiction of what is happening on-screen. Although Windows Media Player or VLC Player are capable of showing the videos, the program provided by COBAN provides an interface identical to the DVMS software.

Data Replication

Data redundancy is important for every agency in order to guarantee necessary videos and data will not be lost due to server or storage failure. COBAN provides departments the flexibility to decide how they copy videos and data to a secondary source. Local storage, DVDs, Cloud, or even a hybrid solution are all compatible with the COBAN system. Agencies also have the choice to replicate just videos, event based data, or all data according to their policies.

COBAN In-Car Digital System Features

✪ Configurable Triggers	Triggers can be configured using DVMS to define a chain of actions for the in-car system, i.e. initiate recording when the car reaches a certain speed.
✪ Event Data Collection	After each stop, the officer can select from a department defined list of events and enter additional offender information as needed.
✪ Fail Safe Drive	Provides data redundancy within the in-car system in case of crash or catastrophic incident.
✪ Integrate w/ Multiple Devices	Each system has an open architecture design to enable connection to external devices, i.e. speed radar.
✪ Metadata Collection	Each video can synchronize with information such as GPS, radar, speed readings, etc.
✪ Multiple Camera Support	Supports up to 6 camera inputs and up to 5 cameras recording simultaneously.
✪ No Restriction Pre/Post Event Recording	Administrator can configure pre and post-event recording duration, based on agency policy and procedures.
✪ Removable Media	Ruggedized removable SSD that can withstand extreme temperatures, vibration and shock.
✪ Smart Power Management	Power management system that protects and monitors power coming from the vehicle and provides system diagnostics for troubleshooting purposes.
✪ Three Separate Audio Channels	If necessary, users can easily isolate the audio from the user-worn body transmitters and covert in-car mic during playback.

COBAN Back Office System Features

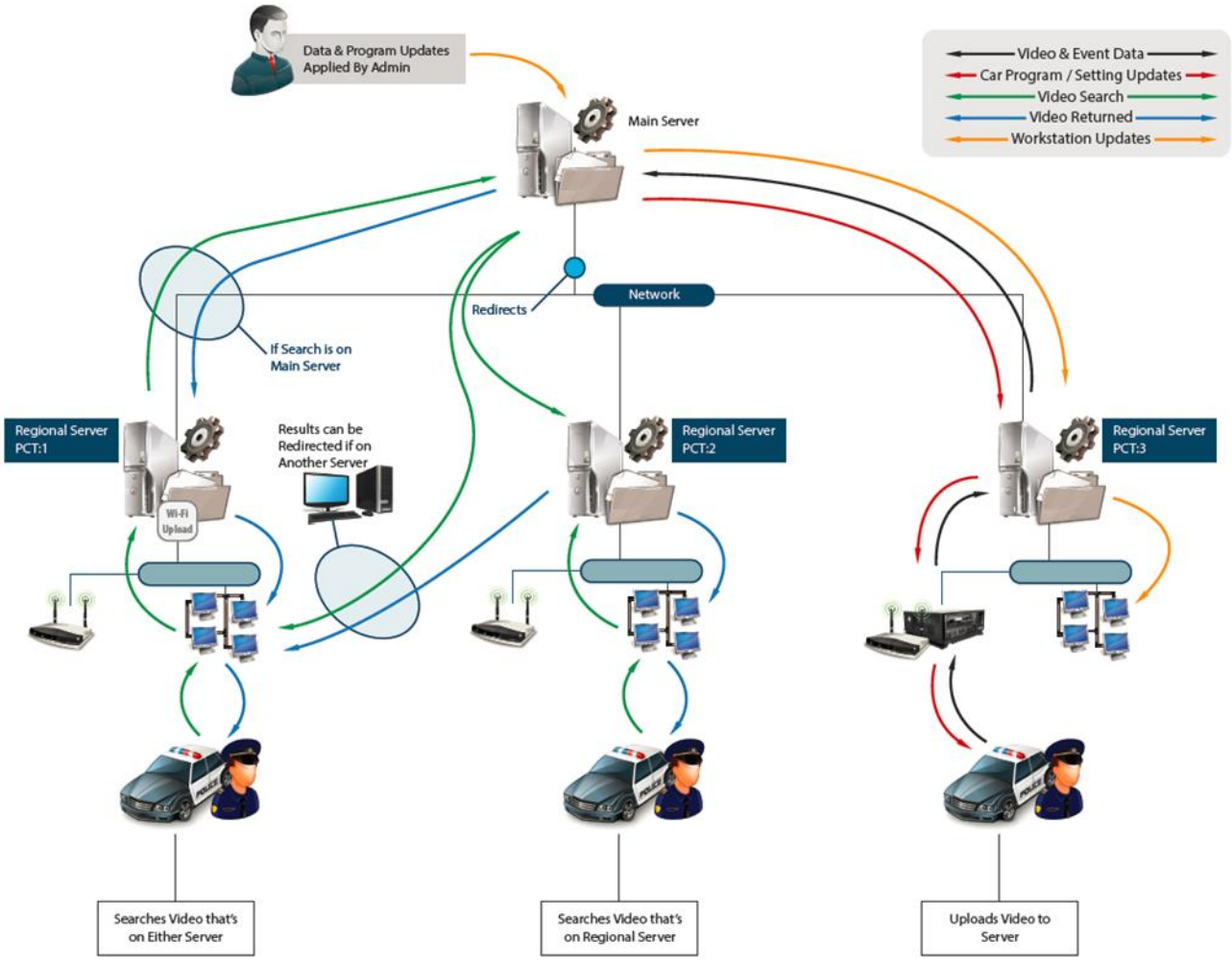
Features	Advantages	Benefits
Centralized In-Car Policy Setting/Automatic Update	By using vehicle templates, admins can set configuration and parameters from a central location. Updates are done concurrently when transferring videos to the station.	Uniform fleet configuration and increased efficiency.
Automatic Video Retention	The system administrator can select which types of videos are archived to the extended storage system. Retention period can also be defined. Once a retention period expires, videos are purged automatically.	Advanced management of video files. Reduction in man hours associated with maintaining videos.
Powerful Search Capability	Expanded search criteria reduces the amount of unnecessary results. Results are immediate.	Increased productivity. No need to request a DVD to view.
Multi-Video Playback	Single incidents that involve recordings from multiple units can be played back simultaneously, synchronized by time. Up to nine videos can be reviewed at once.	Better ability to develop chain of events for courtroom or training purposes.
Versatile Video Export Functions	Allows the department to export to different video formats. CD, Data DVD, or Video DVD. Auto DVD supported feature.	Increase in efficiency. Proprietary video player unnecessary.

COBAN Enterprise Solution is specifically designed for multiple precinct agencies and provides several functions.

1. All data under department domain, including officers, vehicles, and event definitions, can be centrally maintained. A main server acts as a single data maintenance point, and updated data will be pushed to all sub-stations on a daily basis, allowing for consistent data content across all sites.
2. Event data is accumulated at the main server, which then enables query and playback of videos amongst the sub-stations across the network.
3. After program updates for both in-car and backend software are loaded onto the main server, sub-stations will receive the updates automatically.

All of the aforementioned functions do not need to be enabled. Departments can choose which features are most suited for department policy. As an example, if network bandwidth is a concern, videos can be stored at the sub-stations while event data is pushed to the main server. In this instance, even though COBAN is providing distributed storage architecture, an approved user can access any video on the network for the purposes of viewing or exporting. The Enterprise Solution furthers the flexibility, interconnectivity, and network capabilities inherent in COBAN's end-to-end system.

Inter-Precinct Transfer Diagram



COBAN Solution Overview

EDGE Hi-Def

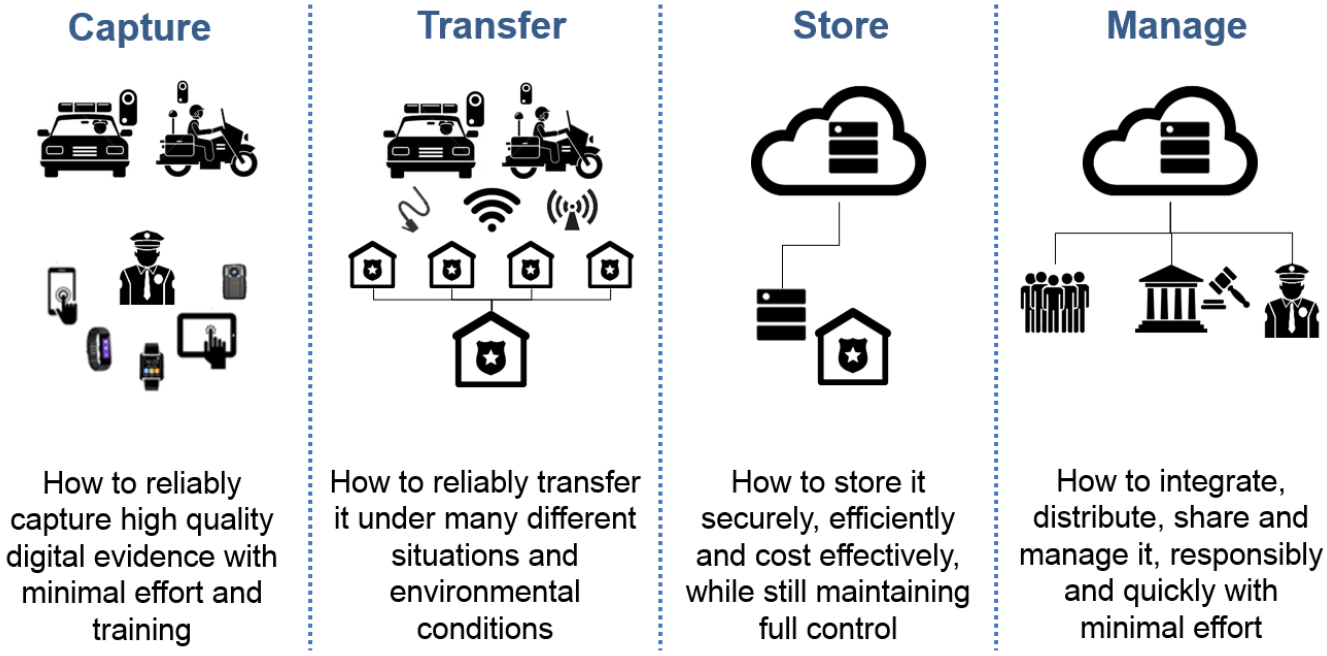
11375 West Sam Houston Parkway South # 800
Houston, Texas 77031

Introduction

The solution proposed by COBAN offers a powerful and varied function set intended for use by law enforcement and public safety industries. The products and services provided by COBAN are modular in design, both in terms of configuration and scale. The following information explains the major functions of our solution and how they will meet your requirements.

COBAN Solutions Overview

There are four phases to digital video projects that form the life cycle of video evidence. This document will describe the flexibility, security, and scalability of COBAN's solutions in regards to these aspects:



Video Capture

COBAN's video capture solutions offer utility that can be scaled and configured to fit the needs of any law enforcement agency. The focus of this overview will be the COBAN EDGE Hi-Def and its related components.

COBAN EDGE Hi-Def

COBAN's EDGE Hi-Def systems are designed as high performance mobile digital video recorders with the understanding that technology requires both usability and capability. EDGE Hi-Def possesses features that are not only intuitive for the user, but easily incorporate into the agency's data management ecosystem. COBAN will also provide MDC Integration software, allowing the officer to control the EDGE HI-Def system via his or her in-car computer. The proceeding information highlights the capabilities of the EDGE Hi-Def.

Multiple-Camera Support

Cameras are the basis for digital video recording. It may seem obvious, but the number and position of cameras are important factors in determining the effectiveness of a system.

The EDGE Hi-Def is capable of supporting up to 6 cameras and several different configurations depending on the department's needs. The local administrator can adjust how the cameras operate by using the back office software provided by COBAN.

Dual-Wireless Microphone

Sound is a significant aspect of any officer related incident. In conjunction with visual evidence, audio recordings give insight to the situation at hand.

EDGE Hi-Def supports two wireless transmitters plus a covert in-car microphone. All three microphones can be controlled separately. The wireless transmitters also have two programmable buttons in addition to the record button. Functions that can be mapped to these buttons include mute, bookmark, camera auto-zoom, stop recording, partner alert, or covert recording.

The partner alert function is used to trigger the partner's transmitter to vibrate and/or light up, dependent upon the back office configuration. If the transmitters are set to covert mode, there will be no response so as to not compromise the officer's position.

The covert recording function allows the officer to remotely begin a rear seat camera recording while blanking out the system's monitor. When suspects are placed in the back seat, they will have no indication that they are being recorded.

Flexible Pre-Event and Post-Event Recording

Pre-event and post-event recording is important in guaranteeing the entirety of an event is captured on video.

The local administrator can configure the desired length of pre- and post-event recording without restrictions. If needed and allowed by policy, the officer may adjust the buffer size while in the car.

Fail-Safe Recording

Fail-safe recording ensures that captured video is retained in case of accidents or localized failure. This is achieved by duplicating all video content to both the CPU's internal drive and the removable hard drive. If for some reason a drive experiences failure, there will always be a backup copy on the other. With this feature, it is less likely that important video is lost due to unforeseen circumstances.

Smart Power Monitoring

Every in-car system offered by COBAN comes with Smart Power Monitoring as a standard function. The hardware module that controls this feature is built into the main CPU unit, so there are no external components beyond a small, replaceable UPS battery.

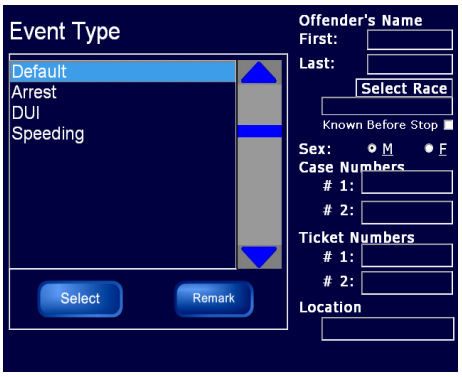
Smart Power Monitoring controls the power transmitted to a system, protecting against damage to both the unit and the car itself. For example, if the voltage provided by the car is insufficient, the system will alert the officer, switch to the backup UPS source, and begin a delayed shutdown process. This prevents the in-car system from draining the car battery and causing software corruption due to improper shutdown.

Smart Power Monitoring also creates a log file that constantly tracks the power readings, system actions, and triggers activated during a shift. The log will be updated from the moment a unit is powered on to the point the system is powered off. This is a useful diagnostic tool in case there are any hardware issues, as it allows insight to the operational environment.

In addition, if there are any possible problems detected, the system can send out an automatic email to notify the proper personnel that maintenance may be required.

Event Data Collection

Event data helps to identify captured video and provides additional incident information.



Data such as the type of offense, offender's information, case numbers, and more can be entered using a keyboard, the touch screen monitor, or magnetic strip reader. This data can be used to attain a more complete understanding of the incident in question, and sort the uploaded videos for easier organization down the line.

Metadata Collection

Metadata provides additional data that may prove helpful in identifying when, where, and how an incident occurred.

Information such as date/time, light bar status, speed radar readings, and GPS coordinates can be recorded automatically through various digital trigger connections. Like event data, this can lead to a more complete understanding of the circumstances surrounding an incident.

Configurable Triggers

Input triggers allow a certain amount of automation once a specific action is initiated. For example, when a patrol car's light bar is activated, triggers may also initiate recording. These are set by the administrator through DVMS, and are included in the metadata associated with a recording.

Snapshot Function

Officers have the capability to capture snapshots using the system's front camera. These snapshots can then be reviewed in the car, exported along with videos, or uploaded separately to servers.

Bookmark Function

Officers can insert "bookmarks" into captured videos during recording or in-car playback. Bookmarks serve as metadata tags after videos are uploaded to the server. When a video is reviewed at a workstation, these bookmarks can be used to jump to a corresponding time point, indicating an important occurrence.

GPS and Mapping Software

GPS is offered as a standard accessory for EDGE Hi-Def systems. COBAN's Digital Video Management Software can use GPS data to highlight a patrol car's physical location, overlaid on a regional map. The mapping function can also be used to initiate video streaming once a patrol car is in specific range. A proper wireless infrastructure must be in place for streaming to happen.

Automated In-Car System Update

In some cases, it may be necessary for administrators to update or modify the user settings of the in-car systems. This can be an overwhelming task if done on an individual unit basis.

COBAN's solution allows for an easy update process. Any settings defined by the system administrator can be transmitted to any in-car unit at the end of a wireless upload or through the process of checking out a removable hard drive.

ECHO Body Worn Camera Integration

The EDGE Hi-Def can be integrated with the COBAN ECHO Body-Worn Camera solution. Users can transfer recorded videos and data directly from the Body-Worn Camera to the in-car unit. The videos and data from both BWC and in-car sources can then be uploaded together, either through wireless or direct transfer via the data infrastructure. Once transferred, the digital evidence will be linked together and managed by the same Digital Video Management System software.

Video Transfer

Video transfer for the EDGE Hi-Def involves video upload, video streaming, and inter-precinct transfer. Transfer is a critical step in the lifecycle of digital video evidence; problems sometimes occur at this stage because of bottlenecking or inefficiencies in infrastructure. COBAN's video transfer solutions are designed to lessen the probability of difficulties and ensure availability of all digital video properties.

Video Upload

COBAN's solution provides three upload methods for flexibility and fail-safe protection. Depending upon an agency's protocol and infrastructure, any one or a combination may suit upload requirements.

Wireless Upload

COBAN's wireless upload method uses 802.11 a/g/n/ac protocol for high speed uploading. The wireless network card is built into the main unit; there are no separate modules required to install.

If, for any reason, an upload session does not complete, a checkpoint transfer algorithm allows the upload to be interrupted and resumed at a later time without having to start over from the beginning. Also, when there are time constraints, specific videos can be selected by the officer for priority upload. The remaining videos will be uploaded at the next available opportunity.

The system administrator can designate how the in-car units access the wireless upload server. Settings can be configured to actively search for the upload server and automatically begin the uploading process once a connection is established, or to upload videos only when the officer explicitly instructs the system to do so.

It is sometimes difficult for agencies to anticipate just how much strain on a network is possible when there are numerous uploads occurring all at once. If wireless upload is a practicable option, COBAN will need to conduct an infrastructure survey to provide recommendations for wireless networks and collaborate with departments to address the possible limitations.

Wired Upload

COBAN's wired upload method uses both 100BASE-T and Gigabit Ethernet network interface. Wired upload is much faster than wireless, but requires cabling and physical stations that will connect the car to the network. Wired upload presents its own set of challenges, and COBAN will consult with the agency regarding equipment specifications, durability, network security, and personnel safety.

Removable Media Upload

COBAN also provides removable, industrial grade Solid State Drives as a functional upload solution. These removable hard drives are encased in a hardened shell for extreme durability and can be transported without fear of physically breaking. For security purposes, the hard drive is only accessible by using a specially designed cradle what will connect to any high-speed USB 2.0 or 3.0 interface. This is the fastest and most efficient method of uploading for departments that have tight turnaround shifts.

Removable hard drives are standard with every COBAN in-car system, and can function as the primary upload system or as a backup method if there are any network issues.

Video Streaming

When an officer initiates event recording, the EDGE Hi-Def can stream videos to the backend dispatch or control center. Any IP based wireless network is compatible, and available bandwidth will directly affect how many FPS are transmitted. If the network bandwidth is not capable of supporting video streaming, the department has the option of transferring live snapshots every few seconds. COBAN's DVMS software is able to simultaneously display up to 16 streaming videos or live images on each workstation's display.

Inter-Precinct Transfer

For departments that have multiple precincts, it is important to have any uploaded videos and data available to all approved users across the network without compromising security. To address this, COBAN provides both centralized and distributed video storage. Dependent upon the department's existing infrastructure and budgeted funds, COBAN will work to recommend the best solution that fits current needs without restricting potential growth.

Even if distributed video storage is used, all the metadata can be pushed to the central server with minimum bandwidth requirement. All authorized users on the department network, no matter the physical location, will be able to locate, playback, and export any video stored on the regional servers.

Video Storage

COBAN offers several types of video storage to accommodate the specific needs of a department, no matter how small or large. In instances where a storage network is already in place, COBAN can work with the agency to ensure compatibility and sustainability. Types of storage we offer include Local Primary Storage, Extended Storage, Cloud storage, and Hybrid solution. The following information details each of these different forms.

Local Primary Storage

Local Primary Storage is when videos are hosted on a nearby server with internal storage or an attached disk array. The videos are available for viewing to whoever possesses the access rights. Local Primary Storage is used when the videos in question have been recently uploaded or will be accessed frequently. Local Primary Storage provides the fastest transfer rates of all the storage options and immediate access to all data located on the server or disk array. At this stage, the department can still maintain complete control over security and ownership of their data.

COBAN can recommend a disk storage system that fits within the department's projected requirements and budget, while maintaining flexibility for future growth. Points to consider when making this recommendation include the amount of video generated on a daily basis and the length of time that videos need to be quickly retrieved on line.

Typically, Local Primary Storage incurs higher initial costs when compared to Cloud or remote storage. However, there are no further usage or access fees after the initial deployment. So for departments with heavy network usage, over longer periods of time, local storage will be the more cost effective choice.

Local Extended Storage

Local Extended Storage is used to retain videos and data for longer durations than Local Primary Storage. This can be anywhere from a few months to years past the department's online requirement. Videos that are not accessed often or marked as critical will be moved from Primary over to Extended Storage for retention purposes. Local Extended Storage may take the form of a secondary server, Network-Attached Storage, Direct-Attached Storage, Storage Area Network, or even DVDs. COBAN's solution provides the flexibility to initiate the required network infrastructure (a server) or expand the department's existing long-term data storage.

COBAN's Auto DVD Solution is an extended storage option that does not require additional IT personnel to operate. It provides a local, on-site solution that incorporates well with any preexisting infrastructure. With Auto DVD Solution, any video matching preconfigured event types are automatically sent to the DVD robot for export. After a DVD is written, it can be retained locally or given to the proper official for courtroom purposes. Anywhere from one to five copies per video can be exported depending upon the department's standard operating procedure. The Auto DVD Solution is designed to eliminate the man hours spent exporting and creating DVDs manually.

Cloud Storage

Cloud Storage is a remote based solution. It involves uploading all captured video and data directly to a remote server where it will be hosted by another party. There is no designation between online and archived data, and if access is required, a video will need to be downloaded from the Cloud server. The appeal of Cloud Storage is that it lessens the need for IT personnel and investment in storage hardware, since there is no need for intermediary local servers. The Cloud is a viable solution for departments that possess robust network bandwidth.

COBAN utilizes industry-leading Microsoft Azure Government for Cloud storage services. Microsoft Azure Government is CJIS capable, FedRAMP compliant, and DISA certified to ensure the security of data. Cloud services do not require separate licenses or access administration and data management are still done within the Digital Video Management system.

While the initial cost of Cloud is much lower than that of local storage, subscription fees and increasing data volume eventually lead to higher than anticipated expenditures. Also, since the Cloud is so heavily dependent on bandwidth, not all agencies will be equipped to realistically implement this type of storage system. It is not a universal solution and COBAN will cooperate with the department to make sure there is a clear understanding of the potential benefits provided by the Cloud.

Hybrid Storage Solution

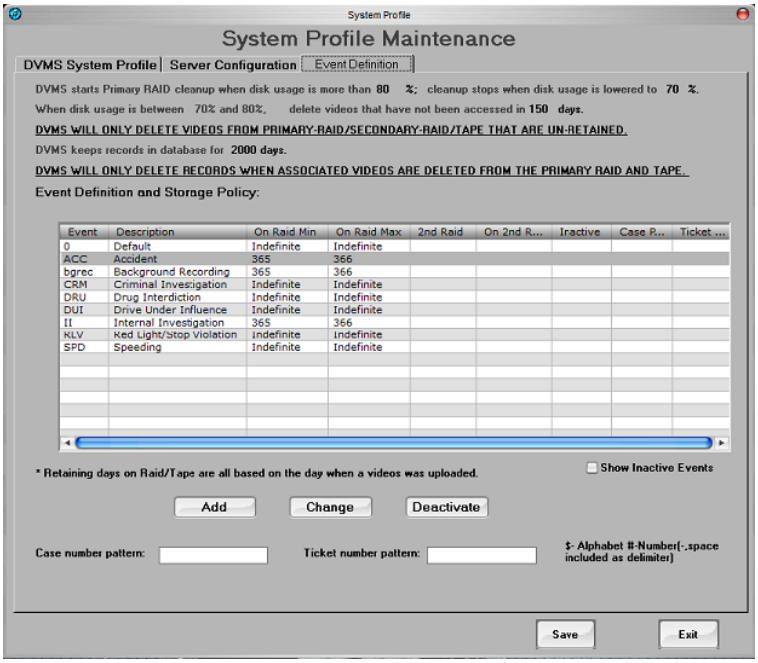
The Hybrid Storage Solution is a partial combination of the concepts behind Local and Cloud storage systems. Rather than immediately pushing all data to the Cloud, videos are initially uploaded to a local gateway. Certain types of videos, in accordance to department policy, can be kept locally for

easier and more immediate retrieval. All other types of videos, or videos that have passed a specified time frame with no deliberate action taken, can then be scheduled for automatic upload to the cloud for retention purposes.

The strength of the hybrid solution is that it can conform to the existing infrastructure to ensure impact on the network is minimized. It is not necessary to acquire multiple servers at one location or augment internet access capabilities. Along these lines, the Hybrid solution decreases the strain on bandwidth when compared to a Cloud solution, as uploads can be arranged to occur at off-peak times instead of all at once, and a copy of high priority event type videos can be kept on the caching device to avoid having to re-download the file for access. The Hybrid solution may not be compatible with a department's needs because it still requires some local infrastructure and IT personnel, while the fees associated with Cloud storage are still applicable, albeit at a lower tier. But for certain departments, dependent upon size and usage, a Hybrid solution has the potential to fit storage requirements while minimizing the necessary investment in new infrastructure. The storage solution provided by COBAN will always comply with each individual agency's resources and requirements. Our aim is to provide a functional and complete solution that will not conflict with the department's budget or capabilities.

Video Management

COBAN's Digital Video Management System is a back office, policy-based automation software that allows administrators to focus on overall system performance instead of day-to-day operational tasks.



Centralized In-Car Policy Setting

The system admin can set up many in-car options through the backend software, including how units respond to input triggers, the functions of the wireless microphone's programmable buttons, the duration of pre-event and post-event recording, and more. Once it has been determined, the settings will be pushed to the in-car units at the end of an upload session or during the process of removable

hard drive checkout. Changes in department policy can be easily implemented for the whole fleet without the need to schedule downtime.

Video Retention

The systems administrator determines how each category of video is handled; retention period for each video is connected to its type. Once the retention period has passed and no deliberate action has been taken, videos are purged from the system automatically. This guarantees policy compliance while minimizing the amount of time spent micromanaging files.

Automated System Management

After the administrator defines the necessary criteria, DVMS will take over the everyday video management jobs. Diagnostic reports will be generated, showing the results of daily tasks and overall storage status. System exceptions are also emailed to alert the system administrator for immediate review.

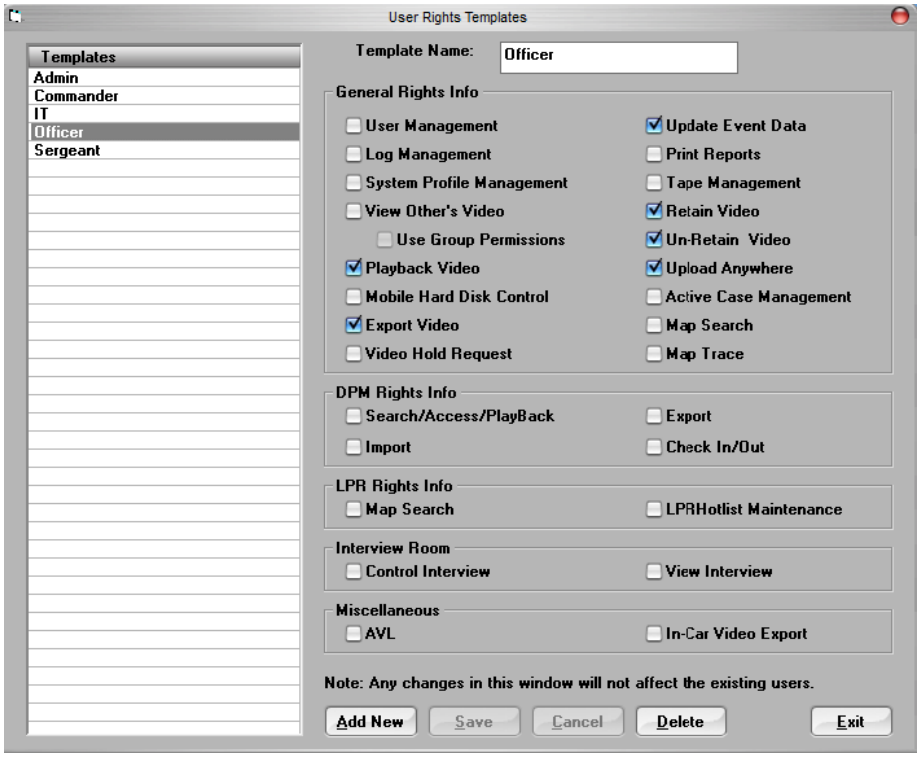
Complete Chain of Custody

At the time of capture, each video is associated with a digital signature that is generated using an MD5 Hash Algorithm, providing integrity verification.

All activities associated with each uploaded video are logged to the system's audit trail. This includes the date and time a video was uploaded, archived, played back, exported, or purged from the system. A complete history of each video is available to the system administrator for analysis.

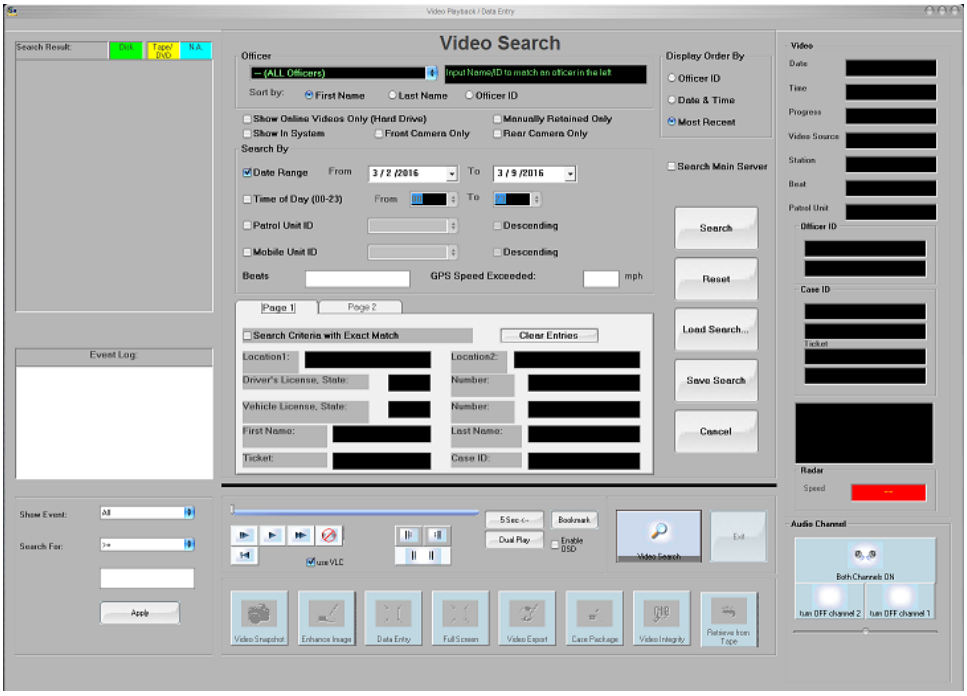
System Security

Activity permissions such as video access, report printing, and general data management functions can be set up by the administrator. Only users with proper clearance are able to perform actions associated with a video in question, and all activities are logged into the aforementioned audit trail.



Powerful Search Capability

Videos can be searched using all event data associated with the in-car units, including offender's ID, patrol unit, event type, time range, and more. The multiple criteria selection allows the user to find specific videos or perform general inquiries.



Centralized Management System

DVMS is capable of managing videos and data from both COBAN Body Worn Cameras and In-Car Video systems. Organization and management of videos involves the same interface and procedures regardless of the source. In addition, associated videos can be grouped together into a case file for easier organization.

Streamlined Storage Management

Whether the department uses Local, Cloud, or Hybrid storage, DVMS provides a standard management system that does not require changes to user interface or external software. Storage server policy, once established by the local system administrator, is automated while still allowing specific videos and data to be handled on an individual basis.

GPS Support

If GPS is implemented, a map interface may be used to search for videos. Also, there is a Route Trace function in DVMS that allows authorized personnel to view the course a car has taken throughout a shift.

Digital Property Manager (DPM)

DPM is value added software that is included within DVMS. It imports, aggregates, and manages externally sourced digital evidence like videos, audio, or documents based on case number.

Users can add external files into the system or link to in-car and interview room videos to form a case package. The system maintains all versions of each individual file in addition to an audit trail to track activity. There is also an export function that allows the user to send all the digital evidence to a DVD, with a searchable index for easy reference.

COBAN Courier

COBAN Courier service allows the department to export videos or Digital Property Management case files without the need for physical DVDs. When the department uploads the requested video, a link will be sent via email to the intended recipient so he or she may access/download it. The link is time-sensitive and the duration can be configured as necessary. Although Courier service is Cloud based, it does not require a COBAN Cloud subscription to be available for use.

Distributable Video Playback Tool

When videos are transferred to DVD or other portable media, DVMS can include an installation program for playback viewing. The program will install a video playback tool on any Windows XP, Vista, 7, or 10 based computers. All the event data present will be displayed along with the video, giving a more complete depiction of what is happening on-screen. Although Windows Media Player or VLC Player are capable of showing the videos, the program provided by COBAN provides an interface identical to the DVMS software.

Data Replication

Data redundancy is important for every agency in order to guarantee necessary videos and data will not be lost due to server or storage failure. COBAN provides departments the flexibility to decide how they copy videos and data to a secondary source. Local storage, DVDs, Cloud, or even a hybrid solution are all compatible with the COBAN system. Agencies also have the choice to replicate just videos, event based data, or all data according to their policies.

COBAN In-Car Digital System Features

✪ Configurable Triggers	Triggers can be configured using DVMS to define a chain of actions for the in-car system, i.e. initiate recording when the car reaches a certain speed.
✪ Event Data Collection	After each stop, the officer can select from a department defined list of events and enter additional offender information as needed.
✪ Fail Safe Drive	Provides data redundancy within the in-car system in case of crash or catastrophic incident.
✪ Integrate w/ Multiple Devices	Each system has an open architecture design to enable connection to external devices, i.e. speed radar.
✪ Metadata Collection	Each video can synchronize with information such as GPS, radar, speed readings, etc.
✪ Multiple Camera Support	Supports up to 6 camera inputs and up to 5 cameras recording simultaneously.

✪ No Restriction Pre/Post Event Recording	Administrator can configure pre and post-event recording duration, based on agency policy and procedures.
✪ Removable Media	Ruggedized removable SSD that can withstand extreme temperatures, vibration and shock.
✪ Smart Power Management	Power management system that protects and monitors power coming from the vehicle and provides system diagnostics for troubleshooting purposes.
✪ Three Separate Audio Channels	If necessary, users can easily isolate the audio from the user-worn body transmitters and covert in-car mic during playback.

COBAN Back Office System Features

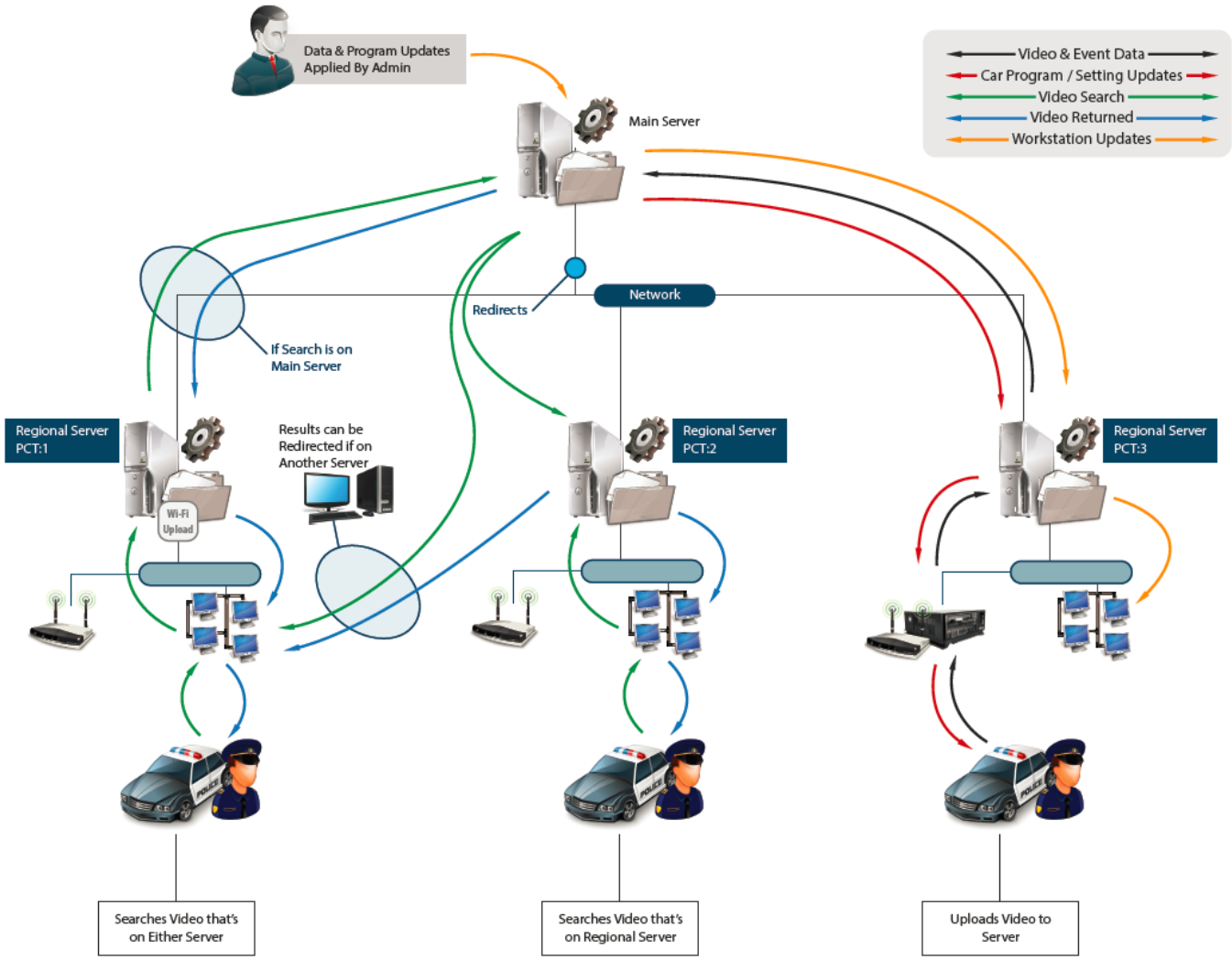
Features	Advantages	Benefits
Centralized In-Car Policy Setting/Automatic Update	By using vehicle templates, admins can set configuration and parameters from a central location. Updates are done concurrently when transferring videos to the station.	Uniform fleet configuration and increased efficiency.
Automatic Video Retention	The system administrator can select which types of videos are archived to the extended storage system. Retention period can also be defined. Once a retention period expires, videos are purged automatically.	Advanced management of video files. Reduction in man hours associated with maintaining videos.
Powerful Search Capability	Expanded search criteria reduces the amount of unnecessary results. Results are immediate.	Increased productivity. No need to request a DVD to view.
Multi-Video Playback	Single incidents that involve recordings from multiple units can be played back simultaneously, synchronized by time. Up to nine videos can be reviewed at once.	Better ability to develop chain of events for courtroom or training purposes.
Versatile Video Export Functions	Allows the department to export to different video formats. CD, Data DVD, or Video DVD. Auto DVD supported feature.	Increase in efficiency. Proprietary video player unnecessary.

COBAN Enterprise Solution is specifically designed for multiple precinct agencies and provides several functions.

1. All data under department domain, including officers, vehicles, and event definitions, can be centrally maintained. A main server acts as a single data maintenance point, and updated data will be pushed to all sub-stations on a daily basis, allowing for consistent data content across all sites.
2. Event data is accumulated at the main server, which then enables query and playback of videos amongst the sub-stations across the network.
3. After program updates for both in-car and backend software are loaded onto the main server, sub-stations will receive the updates automatically.

All of the aforementioned functions do not need to be enabled. Departments can choose which features are most suited for department policy. As an example, if network bandwidth is a concern, videos can be stored at the sub-stations while event data is pushed to the main server. In this instance, even though COBAN is providing distributed storage architecture, an approved user can access any video on the network for the purposes of viewing or exporting. The Enterprise Solution furthers the flexibility, interconnectivity, and network capabilities inherent in COBAN's end-to-end system.

Inter-Precinct Transfer Diagram



COBAN Solution Overview

FUSION HD

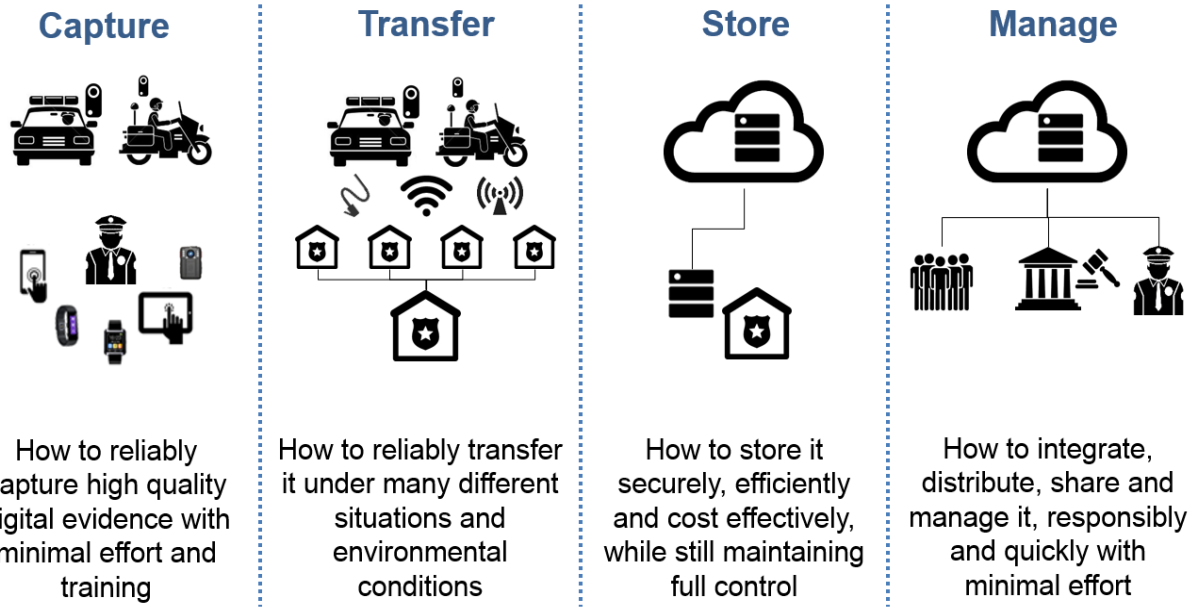
11375 West Sam Houston Parkway South # 800
Houston, Texas 77031

Introduction

The solution proposed by COBAN offers a powerful and varied function set intended for use by law enforcement and public safety industries. The products and services provided by COBAN are modular in design, both in terms of configuration and scale. The following information explains the major functions of our solution and how they will meet your requirements.

COBAN Solutions Overview

There are four phases to digital video projects that form the life cycle of video evidence. This document will describe the flexibility, security, and scalability of COBAN's solutions in regards to these aspects:



Video Capture

COBAN's video capture solutions offer utility that can be scaled and configured to fit the needs of any law enforcement agency. The focus of this overview will be the COBAN FUSION HD and its related components.

COBAN FUSION HD

COBAN's FUSION HD systems are designed as high performance mobile digital video recorders with the understanding that technology requires both usability and capability. FUSION HD possesses features that are not only intuitive for the user, but easily incorporate into the agency's data management ecosystem. The proceeding information highlights the capabilities of the FUSION HD.

Compact All-In-One Design

The FUSION HD is a single module that mounts adjacent to a vehicle's windshield. All the standard components, from the front-facing camera to the screen to the microphone receiver, are integrated into the unit; only the optional rear-facing IR camera and wireless network module are separate. This design minimizes the physical profile of the system while also reducing the amount of cabling necessary for operation. Because of this, installation and uninstallation is simplified when compared to standard in-car video systems.

Multiple-Camera Support

Cameras are the basis for digital video recording. It may seem obvious, but the number and position of cameras are important factors in determining the effectiveness of a system.

The FUSION HD is capable of supporting up to 2 video cameras, with one built-in, front facing HD camera (720p) and an optional rear-facing, wide angle IR camera. It also comes with a built-in

snapshot camera that can be used to capture pictures of license plates, persons-of-interest, or crime scenes. The snapshots taken can then be viewed in the car, uploaded, and exported with corresponding videos if necessary.

Dual-Wireless Microphone

Sound is a significant aspect of any officer related incident. In conjunction with visual evidence, audio recordings give insight to the situation at hand.

FUSION HD supports two wireless transmitters plus a covert in-car microphone. All three microphones can be controlled separately. The wireless transmitters also have two programmable buttons in addition to the record button. Functions that can be mapped to these buttons include mute, bookmark, stop recording, partner alert, or covert recording.

The partner alert function is used to trigger the partner's transmitter to vibrate and/or light up, dependent upon the back office configuration. If the transmitters are set to covert mode, there will be no response so as to not compromise the officer's position.

The covert recording function allows the officer to remotely begin a rear seat camera recording while blanking out the system's monitor. When suspects are placed in the back seat, they will have no indication that they are being recorded.

Flexible Pre-Event and Post-Event Recording

Pre-event and post-event recording is important in guaranteeing the entirety of an event is captured on video.

The local administrator can configure the desired length of pre- and post-event recording without restrictions. If needed and allowed by policy, the officer may adjust the buffer size while in the car.

Fail-Safe Recording

Fail-safe recording ensures that captured video is retained in case of accidents or localized failure. This is achieved by duplicating all video content to both the CPU's internal drive and the removable hard drive. If for some reason a drive experiences failure, there will always be a backup copy on the other. With this feature, it is less likely that important video is lost due to unforeseen circumstances.

Smart Power Monitoring

Every in-car system offered by COBAN comes with Smart Power Monitoring as a standard function. The hardware module that controls this feature is built into the main CPU unit, so there are no external components related to power management. There is also a replaceable internal battery that serves as an emergency Uninterruptable Power Supply.

Smart Power Monitoring controls the power transmitted to a system, protecting against damage to both the unit and the car itself. For example, if the voltage provided by the car is insufficient, the system will alert the officer, switch to the internal backup battery, and begin a delayed shutdown process. This prevents the in-car system from draining the car battery and causing software corruption due to improper shutdown.

Smart Power Monitoring also creates a log file that constantly tracks the power readings, system actions, and triggers activated during a shift. The log will be updated from the moment a unit is powered on to the point the system is powered off. This is a useful diagnostic tool in case there are any hardware issues, as it allows insight to the operational environment.

In addition, if there are any possible problems detected, the system can send out an automatic email to notify the proper personnel that maintenance may be required.

Event Data Collection

Event data helps to identify captured video and provides additional incident information.

Data such as the type of offense, offender's information, case numbers, and more can be entered using the touch screen monitor. This data can be used to attain a more complete understanding of the incident in question, and sort the uploaded videos for easier organization down the line.

Metadata Collection

Metadata provides additional data that may prove helpful in identifying when, where, and how an incident occurred.

Information such as date/time, light bar status, speed radar readings, and GPS coordinates can be recorded automatically through various digital trigger connections. Like event data, this can lead to a more complete understanding of the circumstances surrounding an incident.

Configurable Triggers

Input triggers allow a certain amount of automation once a specific action is initiated. For example, when a patrol car's light bar is activated, triggers may also initiate recording. These are set by the administrator through DVMS, and are included in the metadata associated with a recording.

Bookmark Function

Officers can insert "bookmarks" into captured videos during recording or in-car playback. Bookmarks serve as metadata tags after videos are uploaded to the server. When a video is reviewed at a workstation, these bookmarks can be used to jump to a corresponding time point, indicating an important occurrence.

GPS and Mapping Software

GPS is offered as a standard accessory for FUSION HD systems. COBAN's Digital Video Management System software can use GPS data to highlight a patrol car's physical location, overlaid on a regional map. GPS metadata may also be displayed as information on the video, with coordinates and speed reading visible during playback.

Automated In-Car System Update

In some cases, it may be necessary for administrators to update or modify the user settings of the in-car systems. This can be an overwhelming task if done on an individual unit basis.

COBAN's solution allows an easy update process. Any settings defined by the system administrator can be transmitted to any in-car unit at the end of a wireless upload or through the process of checking out a removable hard drive.

Video Transfer

Video transfer for the FUSION HD involves video upload and inter-precinct transfer. Transfer is a critical step in the lifecycle of digital video evidence; problems sometimes occur at this stage because of bottlenecking or inefficiencies in infrastructure. COBAN's video transfer solutions are designed to lessen the probability of difficulties and ensure availability of all digital video properties.

Video Upload

COBAN's solution provides two upload methods for flexibility and fail-safe protection. Depending upon an agency's protocol and infrastructure, any one or a combination may suit upload requirements.

Wireless Upload

COBAN's optional wireless upload method uses 802.11 a/g/n protocol for high speed uploading. It requires an external module that connects through the LAN port on the unit.

If, for any reason, an upload session does not complete, a checkpoint transfer algorithm allows the upload to be interrupted and resumed at a later time without having to start over from the beginning. Also, when there are time constraints, specific videos can be selected by the officer for priority upload. The remaining videos will be uploaded at the next available opportunity.

The system administrator can designate how the in-car units access the wireless upload server. Settings can be configured to actively search for the upload server and automatically begin the uploading process once a connection is established, or to upload videos only when the officer explicitly instructs the system to do so.

It is sometimes difficult for agencies to anticipate just how much strain on a network is possible when there are numerous uploads occurring all at once. If wireless upload is a practicable option, COBAN will need to conduct an infrastructure survey to provide recommendations for wireless networks and collaborate with departments to address the possible limitations.

Removable Media Upload

COBAN also provides a removable, industrial grade Solid State Pen Drive as a practical upload solution. The pen drives are encased in a hardened shell for added durability. This is the fastest and most efficient method of uploading for departments that have tight turnaround shifts.

Removable pen drives are standard with every COBAN in-car system, and can function as the primary upload system or as a backup method if there are any network issues.

Inter-Precinct Transfer

For departments that have multiple precincts, it is important to have any uploaded videos and data available to all approved users across the network without compromising security. To address this, COBAN provides both centralized and distributed video storage. Dependent upon the department's

existing infrastructure and budgeted funds, COBAN will work to recommend the best solution that fits current needs without restricting potential growth.

Even if distributed video storage is used, all the metadata can be pushed to the central server with minimum bandwidth requirement. All authorized users on the department network, no matter the physical location, will be able to locate, playback, and export any video stored on the regional servers.

Video Storage

COBAN offers several types of video storage to accommodate the specific needs of a department, no matter how small or large. In instances where a storage network is already in place, COBAN can work with the agency to ensure compatibility and sustainability. Types of storage we offer include Local Primary Storage, Extended Storage, Cloud storage, and Hybrid solution. The following information details each of these different forms.

Local Primary Storage

Local Primary Storage is when videos are hosted on a nearby server with internal storage or an attached disk array. The videos are available for viewing to whoever possesses the access rights. Local Primary Storage is used when the videos in question have been recently uploaded or will be accessed frequently. Local Primary Storage provides the fastest transfer rates of all the storage options and immediate access to all data located on the server or disk array. At this stage, the department can still maintain complete control over security and ownership of their data.

COBAN can recommend a disk storage system that fits within the department's projected requirements and budget, while maintaining flexibility for future growth. Points to consider when making this recommendation include the amount of video generated on a daily basis and the length of time that videos need to be quickly retrieved on line.

Typically, Local Primary Storage incurs higher initial costs when compared to Cloud or remote storage. However, there are no further usage or access fees after the initial deployment. So for departments with heavy network usage, over longer periods of time, local storage will be the more cost effective choice.

Local Extended Storage

Local Extended Storage is used to retain videos and data for longer durations than Local Primary Storage. This can be anywhere from a few months to years past the department's online requirement. Videos that are not accessed often or marked as critical will be moved from Primary over to Extended Storage for retention purposes. Local Extended Storage may take the form of a secondary server, Network-Attached Storage, Direct-Attached Storage, Storage Area Network, or even DVDs. COBAN's solution provides the flexibility to initiate the required network infrastructure (a server) or expand the department's existing long-term data storage.

COBAN's Auto DVD Solution is an extended storage option that does not require additional IT personnel to operate. It provides a local, on-site solution that incorporates well with any preexisting infrastructure. With Auto DVD Solution, any video matching preconfigured event types are automatically sent to the DVD robot for export. After a DVD is written, it can be retained locally or given to the proper official for courtroom purposes. Anywhere from one to five copies per video

can be exported depending upon the department's standard operating procedure. The Auto DVD Solution is designed to eliminate the man hours spent exporting and creating DVDs manually.

Cloud Storage

Cloud Storage is a remote based solution. It involves uploading all captured video and data directly to a remote server where it will be hosted by another party. There is no designation between online and archived data, and if access is required, a video will need to be downloaded from the Cloud server. The appeal of Cloud Storage is that it lessens the need for IT personnel and investment in storage hardware, since there is no need for intermediary local servers. The Cloud is a viable solution for departments that possess robust network bandwidth.

While the initial cost of Cloud is much lower than that of local storage, subscription fees and increasing data volume eventually lead to higher than anticipated expenditures. Also, since the Cloud is so heavily dependent on bandwidth, not all agencies will be equipped to realistically implement this type of storage system. It is not a universal solution and COBAN will cooperate with the department to make sure there is a clear understanding of the potential benefits provided by the Cloud.

Hybrid Storage Solution

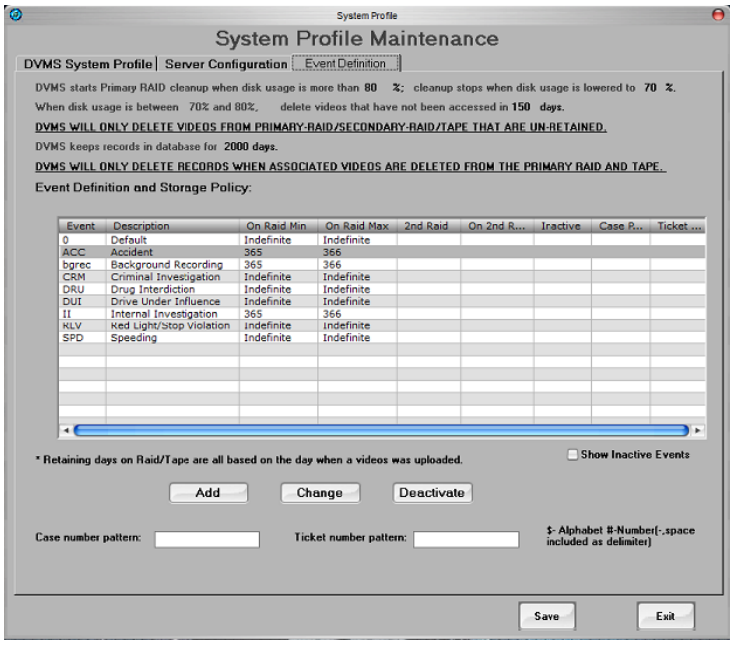
The Hybrid Storage Solution is a partial combination of the concepts behind Local and Cloud storage systems. Rather than immediately pushing all data to the Cloud, videos are initially uploaded to a local gateway. Certain types of videos, in accordance to department policy, can be kept locally for easier and more immediate retrieval. All other types of videos, or videos that have passed a specified time frame with no deliberate action taken, can then be scheduled for automatic upload to the cloud for retention purposes.

The strength of the hybrid solution is that it can conform to the existing infrastructure to ensure impact on the network is minimized. It may not be necessary to acquire multiple servers or augment internet access capabilities. Along these lines, the Hybrid solution decreases the strain on bandwidth when compared to a Cloud solution, as uploads are arranged to occur at off-peak times instead of all at once. The Hybrid solution may not be compatible with a department's needs because it still requires some local infrastructure and IT personnel, while the fees associated with Cloud storage are still applicable, albeit at a lower tier. But for certain departments, dependent upon size and usage, a Hybrid solution has the potential to fit storage requirements while minimizing the necessary investment in new infrastructure.

The storage solution provided by COBAN will always comply with each individual agency's resources and requirements. Our aim is to provide a functional and complete solution that will not conflict with the department's budget or capabilities.

Video Management

COBAN's Digital Video Management System is a back office, policy-based automation software that allows administrators to focus on overall system performance instead of day-to-day operational tasks.



Centralized In-Car Policy Setting

The system admin can set up many in-car options through the backend software, including how units respond to input triggers, the functions of the wireless microphone's programmable buttons, the duration of pre-event and post-event recording, and more. Once it has been determined, the settings will be pushed to the in-car units at the end of an upload session or during the process of removable hard drive checkout. Changes in department policy can be easily implemented for the whole fleet without the need to schedule downtime.

Video Retention

The systems administrator determines how each category of video is handled; retention period for each video is connected to its type. Once the retention period has passed and no deliberate action has been taken, videos are purged from the system automatically. This guarantees policy compliance while minimizing the amount of time spent micromanaging files.

Automated System Management

After the administrator defines the necessary criteria, DVMS will take over the everyday video management jobs. Diagnostic reports will be generated, showing the results of daily tasks and overall storage status. System exceptions are also emailed to alert the system administrator for immediate review.

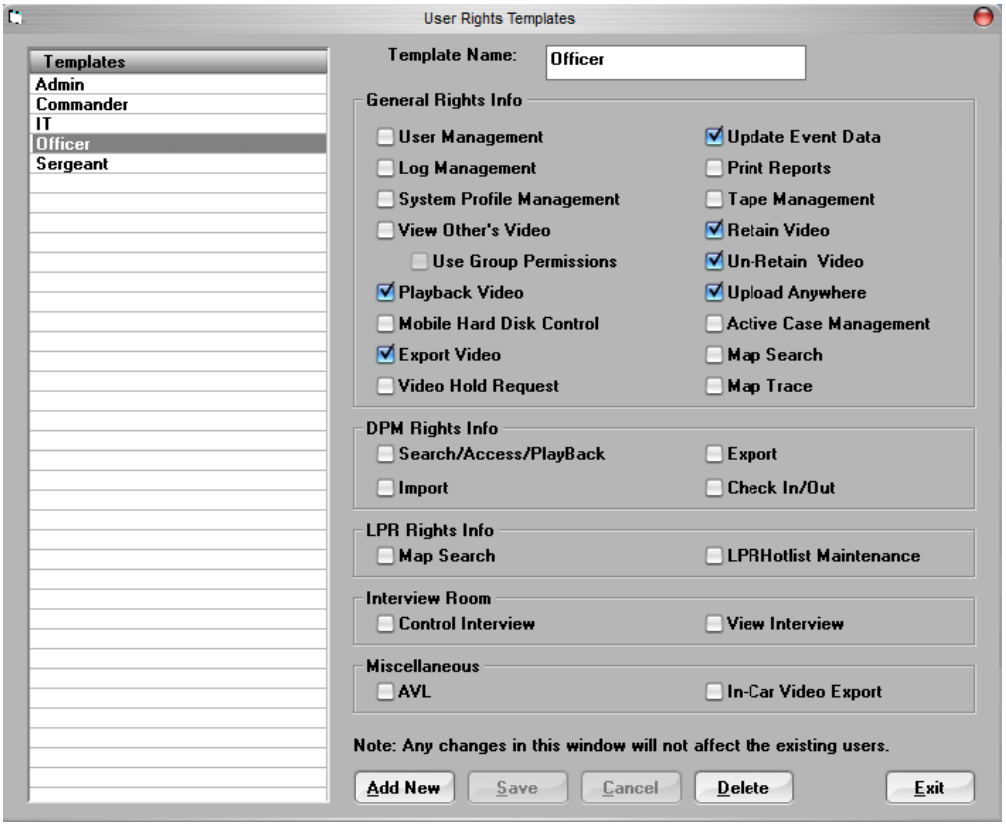
Complete Chain of Custody

At the time of capture, each video is associated with a digital signature that is generated using an MD5 Hash Algorithm, providing integrity verification.

All activities associated with each uploaded video are logged to the system's audit trail. This includes the date and time a video was uploaded, archived, played back, exported, or purged from the system. A complete history of each video is available to the system administrator for analysis.

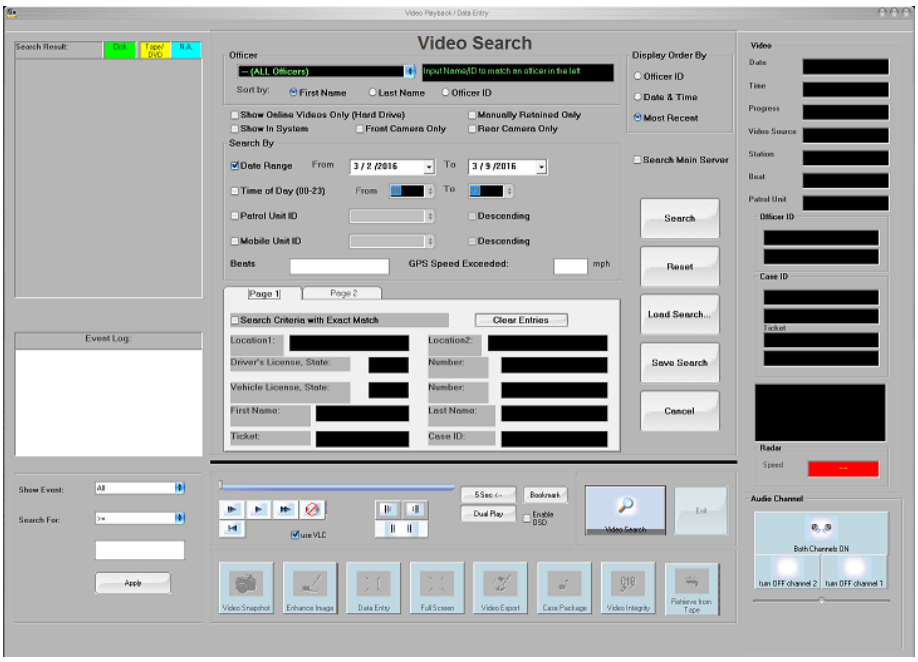
System Security

Activity permissions such as video access, report printing, and general data management functions can be set up by the administrator. Only users with proper clearance are able to perform actions associated with a video in question, and all activities are logged into the aforementioned audit trail.



Powerful Search Capability

Videos can be searched using all event data associated with the in-car units, including offender's ID, patrol unit, event type, time range, and more. The multiple criteria selection allows the user to find specific videos or perform general inquiries.



GPS Support

If GPS is implemented, a map interface may be used to search for videos. Also, there is a Route Trace function in DVMS that allows authorized personnel to view the course a car has taken throughout a shift.

Digital Property Management (DPM)

DPM is value added software that is included within DVMS. It imports, aggregates, and manages externally sourced digital evidence like videos, audio, or documents based on case number.

Users can add external files into the system or link to in-car and interview room videos to form a case package. The system maintains all versions of each individual file in addition to an audit trail to track activity. There is also an export function that allows the user to send all the digital evidence to a DVD, with a searchable index for easy reference.

COBAN Courier

COBAN Courier service allows the department to export videos or Digital Property Management case files without the need for physical DVDs. When the department uploads the requested video, a link will be sent via email to the intended recipient so he or she may access/download it. The link is time-sensitive and the duration can be configured as necessary. Although Courier service is Cloud based, it does not require a COBAN Cloud subscription to be available for use.

Distributable Video Playback Tool

When videos are transferred to DVD or other portable media, DVMS can include an installation program for playback viewing. The program will install a video playback tool on any Windows XP, Vista, 7, or 10 based computers. All the event data present will be displayed along with the video, giving a more complete depiction of what is happening on-screen. Although Windows Media Player or VLC Player are capable of showing the videos, the program provided by COBAN provides an interface identical to the DVMS software.

Data Replication

Data redundancy is important for every agency in order to guarantee necessary videos and data will not be lost due to server or storage failure. COBAN provides departments the flexibility to decide how they copy videos and data to a secondary source. Local storage, DVDs, Cloud, or even a hybrid solution are all compatible with the COBAN system. Agencies also have the choice to replicate just videos, event based data, or all data according to their policies.

COBAN In-Car Digital System Features

✪ Configurable Triggers	Triggers can be configured using DVMS to define a chain of actions for the in-car system, i.e. initiate recording when the car reaches a certain speed.
✪ Event Data Collection	After each stop, the officer can select from a department defined list of events and enter additional offender information as needed.
✪ Fail Safe Drive	Provides data redundancy within the in-car system in case of crash or catastrophic incident.
✪ Metadata Collection	Each video can synchronize with information such as GPS, radar, speed readings, etc.
✪ Multiple Camera Support	Supports up to 2 cameras recording simultaneously.
✪ No Restriction Pre/Post Event Recording	Administrator can configure pre and post-event recording duration, based on agency policy and procedures.
✪ Removable Media	Removable SSD Pen Drive that can withstand extreme temperatures and vibration.
✪ Smart Power Management	Power management system that protects and monitors power coming from the vehicle and provides system diagnostics for troubleshooting purposes.
✪ Three Separate Audio Channels	If necessary, users can easily isolate the audio from the user-worn body transmitters and covert in-car mic during playback.

COBAN Back Office System Features

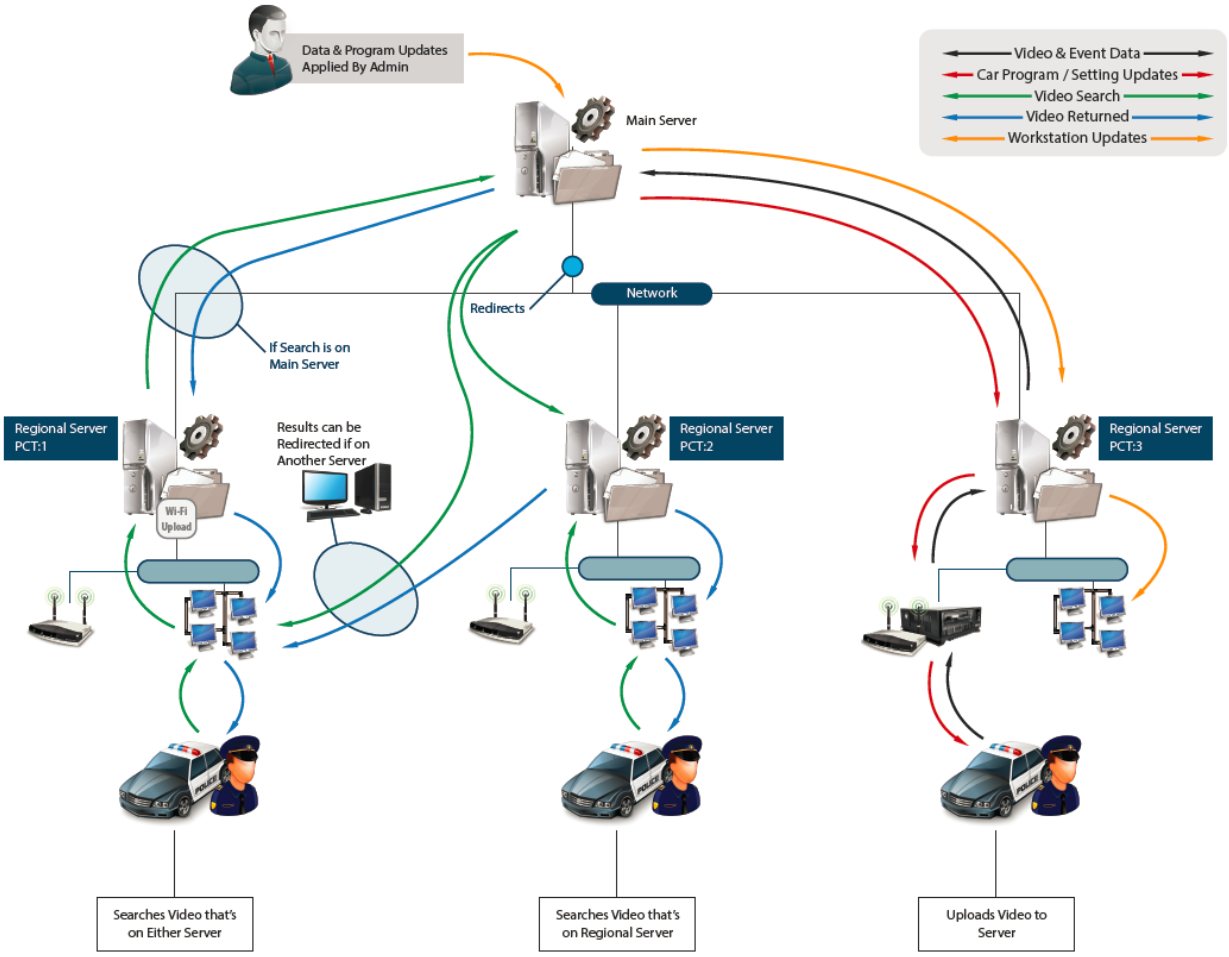
Features	Advantages	Benefits
Centralized In-Car Policy Setting/Automatic Update	By using vehicle templates, admins can set configuration and parameters from a central location. Updates are done concurrently when transferring videos to the station.	Uniform fleet configuration and increased efficiency.
Automatic Video Retention	The system administrator can select which types of videos are archived to the extended storage system. Retention period can also be defined. Once a retention period expires, videos are purged automatically.	Advanced management of video files. Reduction in man hours associated with maintaining videos.
Powerful Search Capability	Expanded search criteria reduces the amount of unnecessary results. Results are immediate.	Increased productivity. No need to request a DVD to view.
Versatile Video Export Functions	Allows the department to export to different video formats. CD, Data DVD, or Video DVD. Auto DVD supported feature.	Increase in efficiency. Proprietary video player unnecessary.

COBAN Enterprise Solution is specifically designed for multiple precinct agencies and provides several functions.

1. All data under department domain, including officers, vehicles, and event definitions, can be centrally maintained. A main server acts as a single data maintenance point, and updated data will be pushed to all sub-stations on a daily basis, allowing for consistent data content across all sites.
2. Event data is accumulated at the main server, which then enables query and playback of videos amongst the sub-stations across the network.
3. After program updates for both in-car and backend software are loaded onto the main server, sub-stations will receive the updates automatically.

All of the aforementioned functions do not need to be enabled. Departments can choose which features are most suited for department policy. As an example, if network bandwidth is a concern, videos can be stored at the sub-stations while event data is pushed to the main server. In this instance, even though COBAN is providing distributed storage architecture, an approved user can access any video on the network for the purposes of viewing or exporting. The Enterprise Solution furthers the flexibility, interconnectivity, and network capabilities inherent in COBAN's end-to-end system.

Inter-Precinct Transfer Diagram



ECHO

Powered by COBAN

- High-Definition Video 720p
- Tested IP56 Water Resistance
- POGO Transfer More Durable Than USB

KEY FEATURES

- **Small/Compact/Lightweight**
- **Multiple Mounting Options**
- **Full Shift Battery Life**
- **On-Camera Event Tagging**
- **Secure Access for Storage**
- **Adjustable Pre-Event Recording**
- **Optional External IR Camera**
- **POGO Sync: Charging / Video Transfer**

ADVANCED DOCKING OPTIONS

MULTI-BAY OFFICE DOCK

- Charges, updates, and uploads
- Videos are automatically transferred

SINGLE-BAY OFFICE/VEHICLE DOCK

- Connect to existing in-car computer to review videos

MANAGE

COBAN COMMAND CENTER
COMMAND CENTER EXPRESS
DVMS Digital Video Management System

ECHO SPECIFICATIONS

Video:	1080P/720P/D1
	Night Mode (0 lux w/IR illuminator)
Pre-Event Mode:	Yes
Angle of View (Main):	110 Degrees
External IR Camera:	90 Degrees
Battery:	8.5 hours record time
	16 hours standby
Storage:	32 GB
Buttons:	Record/Tag/Flashlight
Connections:	POGO (quick contacts) / USB
Warranty:	1 year (2nd/3rd year extended options)
Docking Options:	6 Bay uploading/charging dock
	Single-Bay charging dock (office/vehicle)

ECHO
Powered by COBAN

ADVANCED DOCKING OPTIONS

VIDEO TRANSFER

MULTI-BAY OFFICE DOCK

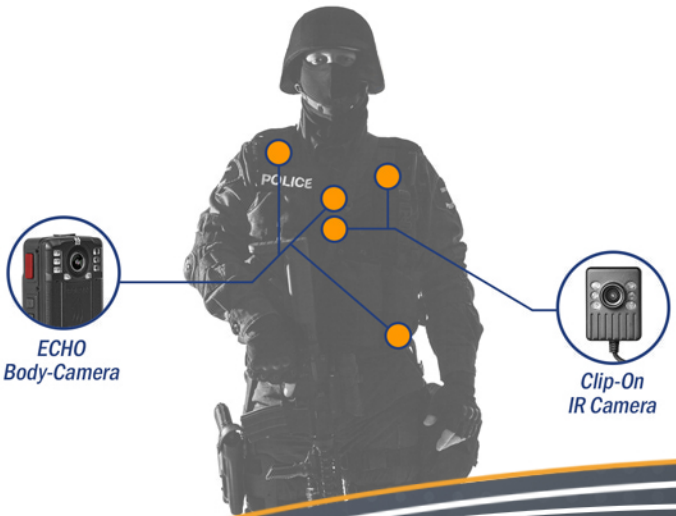
- Charges, updates, and uploads
- Videos are automatically transferred

SINGLE-BAY OFFICE/VEHICLE DOCK

- Connect to existing in-car computer to review videos

SMALL / COMPACT / LIGHTWEIGHT

ECHO packs a lot of punch in a small package. Its 3-2-1 dimensions make it easy to wear without sacrificing functionality or durability. And at just over 4 ounces, ECHO won't weigh you down.



MULTIPLE MOUNTING OPTIONS

ECHO's compact design and flexible fastening system allows you to mount the camera almost anywhere, including the chest, epaulet, or hip.

EDGE SD

Powered by COBAN

CAMERA OPTIONS

STANDARD CAMERA

- 18X Optical Zoom
- 12X Digital Zoom
- .7 Lux
- 48 Deg. Field of View
- 68 Deg. Field of View (opt.)

REAR CAMERA

- IR Camera
- 0 Lux
- 130 Deg. Field of View

MONITOR

- 5.7" LED back light TFT LCD panel with Touch Screen

SYSTEM

- 64GB Solid State Internal Storage
- 64GB Solid State Removable Storage
- 8GB Solid State OS Storage
- Built-in 802.11 a/g/n/ac
- Built-in Crash Sensors
- GPS Receiver and Antenna
- RS-232 Port X 1
- USB 2.0 X 3
- USB 3.0 X 2
- Digital Inputs: Ignition, Light Bar, Ignition, Brake, and General Digital Input
- RJ45 x 2
- Records up to 5 cameras simultaneously

AUDIO

- 900 Mhz Digital Spread Spectrum
- 3 separate audio channels (two transmitters/one back seat microphone)
- Two Programmable Buttons
- 20 Hours Talk Time

Full 3-year hardware warranty.

[1]MIL-STD-810G, the highest standard for mobile equipment in our industry

KEY FEATURES

CAMERA FEATURES

- Up to 6 Cameras
- 18x Optical Zoom
- Less than 1 Lux
- 48° Viewing Angle

MICROPHONE FEATURES

- 900 MHz for least interference
- Clear up to 1000'
- Up to 20 hours Talk Time
- Multichannel with Auto Synchronization
- Rechargeable Lithium-Ion Battery
- 7-Day Standby Time

MONITOR FEATURES

- Sunlight Readable
- Glove Friendly Buttons
- Anti-Glare

Video Solutions for Vehicles

5.7" Touchscreen Monitor
User-friendly interface designed for easy operation. Easily tag videos with the correct ID and enter data after a stop.

Triple Drive Solid State Architecture
COBAN utilizes high performance, industrial grade, solid-state drives that feature no moving parts, eliminating the chance that bumps in the road or the vehicle vibrations will affect the high definition video recording. With over a decade of experience, COBAN has perfected the rugged removable drive based on the unique needs of law enforcement.

Hands-Free System Updates
Wireless download (or removable drive) for software updates or system settings reduces the chance of human error and eliminates downtime during updates.

FailSafe
The highest availability of video evidence out there: dual stream, fail-safe recording. Video is captured twice onto two independent drives. We've got your back.

Smart Power Module
With sophisticated power management and built-in uninterrupted power supply (UPS), Smart Power Module regulates vehicle voltage, and protects your battery and the system's own power supply.

Video Streaming Enabled
No additional hardware necessary. (Requires 4G connection and proper bandwidth.)

Wireless Capabilities
(802.11 a/g/n and optional WiMax). Multiple standards provide flexibility for uploading and wireless updates.

Removable Solid-State Drive
Offers long life cycles and fast read/write speeds. Great choice for video upload when wireless upload is unavailable.

Rugged 900 MHz, Bidirectional, Water-Resistant Mics
Clear to 1000 feet, talk time up to 10 hours. Two agency-defined, programmable buttons offer multiple functions.

Tested and Meets MIL-SPEC-810G
So tough, it meets military specifications (MIL-SPEC-810G). Built to take on the temperature, shock, and vibration of the harsh mobile environment.

Near-Zero Lux Night Mode
Provides clear details for recording video in low light when recording in IR mode.

EDGE HI-DEF

Powered by COBAN

- Three-Year Hardware Warranty
- Tested and Meets MIL-SPEC-810G
- Proven Reliability & Durability
- Built-in Streaming

KEY FEATURES

720p CAMERA FEATURES

- Up to 6 Cameras
- 28x Optical Zoom
- Less than 1 Lux
- 55° Viewing Angle

MICROPHONE FEATURES

- 900 MHz for least interference
- Clear up to 1000'
- Up to 20 hours Talk Time
- Multichannel with Auto Synchronization
- Rechargeable Lithium-Ion Battery
- 7-Day Standby Time

MONITOR FEATURES

- Sunlight Readable
- Glove Friendly Buttons
- Anti-Glare

Video Solutions for Vehicles

5.7" Touchscreen Monitor
User-friendly interface designed for easy operation. Easily tag videos with the correct ID and enter data after a stop.

High-Definition Video Format
Recording video in the most up-to-date industry HD 720p standard means you get better resolution with a wider angle of view.

Hands-Free System Updates
Wireless download (or removable drive) for software updates or system settings reduces the chance of human error and eliminates downtime during updates.

FailSafe
The highest availability of video evidence out there: dual stream, fail-safe recording. Video is captured twice onto two independent drives. We've got your back.

Smart Power Module
With sophisticated power management and built-in uninterrupted power supply (UPS), Smart Power Module regulates vehicle voltage, and protects your battery and the system's own power supply.

Near-Zero Lux Night Mode
Provides clear details for recording video in low light when recording in IR mode.

Video Streaming Enabled
No additional hardware necessary. (Requires 4G connection and proper bandwidth.)

Wireless Capabilities
(802.11 a/g/n and optional WiMax). Multiple standards provide flexibility for uploading and wireless updates.

Removable Solid-State Drive
Offers long life cycles and fast read/write speeds. Great choice for video upload when wireless upload is unavailable.

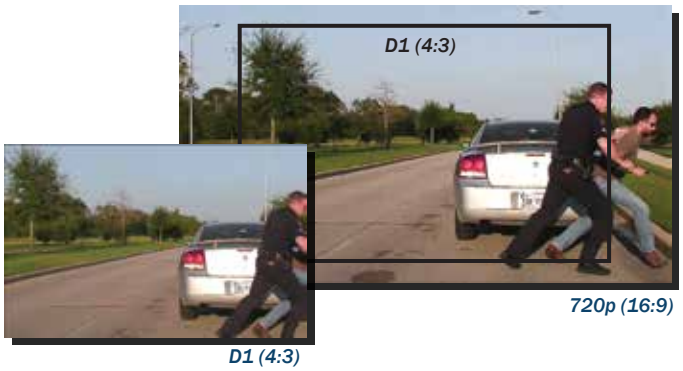
Rugged 900 MHz, Bidirectional, Water-Resistant Mics
Clear to 1000 feet, talk time up to 10 hours. Two agency-defined, programmable buttons offer multiple functions.

Tested and Meets MIL-SPEC-810G
So tough, it meets military specifications (MIL-SPEC-810G). Built to take on the temperature, shock, and vibration of the harsh mobile environment.

FUSION HD

ALL HD, ALL THE TIME!

Let FUSION HD take the burden of video quality selection from your officers. We deliver all high definition video, all the time. **No surprises. No compromise.**



NEVER MISS THE BIGGER PICTURE.

Driver View

Specifications:

- Solid-State Storage
- 4.3” Touch-Screen Display
- Supports Two Wireless Microphones
- Dual Camera Design - Video & Snapshot
- Security Lock for Removable Media
- Built-In GPS and Crash Sensor
- Custom Programmable Function Button
- Optional Backseat Camera & Microphone
- Optional Wireless Upload (802.11a, g, n)

Front View

FailSafe Technology

Always have a backup. Similar to a black box on an airplane, COBAN Failsafe technology continuously records to the internal drive, while storing event-based videos on the removable drive.

Unlimited Pre-Event Recording

Based on FailSafe technology, officers and administrators can retrieve valuable video footage even days later, no matter what FUSION’s recording status was at the time of the event.

MIL-SPEC 810G CERTIFIED

Rugged Design

Built from the ground up and certified to meet military specifications, COBAN’s rugged solution is designed to withstand the harsh conditions police vehicles encounter in the field.

Intelligent Wireless Microphone Design

Always ready, even when you're not.

- Up to 1,000 ft Range
- 12 Hours Talk Time
- 4 Days Stand-by Time
- 21 Days Hibernation Mode
- Two Custom Programmable Function Buttons

Wireless Microphone in Charging Dock

*Each **FUSION** system supports two wireless microphones. The microphone goes beyond just audio transmitting. In addition to a Record Button, two custom programmable function buttons allow the body-worn microphone to serve as a remote control for the FUSION HD in-car system.*

FUSION HD Powered by COBAN

Turnkey Solutions

PLUG & PLAY SERVER

FUSION HD units are shipped with pre-configured storage and management servers. Our representatives help you select the right server, based on your fleet size, video quality selection, and evidence retention requirements. Just power up the server and it's ready to go.

VIDEO MANAGEMENT

Proven Video Management Software

COBAN has been providing video management software to agencies of all sizes for over ten years. From the time the video is captured to the time it is submitted to court, our complete back-office solution allows you to manage all aspects of video evidence.

Automated Processes

Once the software is configured to your agency's policies it handles the video life-cycle based on set parameters, automatically. It takes the administrative burden away from system managers by logging evidence handling in detail.

Quick Video Export

Integrated software allows you to export videos to CD, DVD or Blu-ray discs quickly and easily, without third party software.

Rapid Exchange Program

We understand that video is critical and down-time can be costly.

The COBAN Rapid Exchange Program is designed to minimize downtime for law enforcement when a repair is needed on a FUSION system. Simply fill out the online RMA form, print the UPS shipping label and ship the system to us. You will receive a replacement system the next business day.*

No red tape. No hassle.

*Next day delivery may vary depending on destination.

COBAN

FROM CAR TO COURT, WE'VE GOT YOUR BACK.

COBAN Technologies, Inc.
11375 W. Sam Houston Parkway S. # 800
Houston, TX 77031

Phone: 1 (281) 925-0488
Toll Free: 1 (866) 812-6226
Fax: 1 (281) 925-0535

www.cobantech.com

DIGITAL VIDEO MANAGEMENT SYSTEM

Powered by COBAN

IN-CAR VIDEOS

BODY-WORN

DVMS

INTERVIEW ROOM

AUTOMATIC VEHICLE LOCATOR

IT'S ALL ABOUT AUTOMATION

- Server, workstation, and in-car unit updates are fully automated.
- Imported videos are automatically sent to auto-DVD burners installed in secured locations.
- Interview room and body-worn videos are automatically associated with in-car videos by incident IDs.
- Storage management is automatic. There is no need to manually reconfigure (by moving videos around) when new storage is added to the system.
- Multi-server search is automatic. One click returns complete results from multiple servers and storage classes.
- COBAN Tape Library solution automates video archival and retrieval, no human intervention necessary.

Solutions for Media Management

Evidence Management
Digital Video Management System (DVMS) handles all video evidence—in-car, interview room, body cam, MDC, AVL, even externally imported videos—using the same department policies. COBAN's rule-based storage solution automates the life-cycle maintenance of video evidence.

Highly Scalable Solution
COBAN customers range from five-car to 1500-car,single/multi-station agencies. DVMS provides the most comprehensive set of features and functions in the industry, yet the preconfigured options allow agencies of all sizes to leave most settings as is, changing only a few to comply with agency specific policies. In most cases, DVMS is ready to use right out of the box.

Meeting Your Storage Needs
DVMS offers multiple storage classes to meet each agency's needs. From RAID or tape library to DR (disaster recovery) storage, we've got you covered.

True Enterprise Solution
When multiple videos related to the same incident are uploaded to the local servers at different substations, these videos become available to all authorized users immediately. With a single search, all related videos are available; there's no guessing about which server a video resides on. A single search is all it takes to access all storage classes; there's no need to repeat the same search for each storage class.

Unlimited Storage Space
The COBAN solution uses industry standard multi-layer storage architectures. Storage options for departments range from Virtual Environments, disk raid systems (SAN, iSCSI, DAS) with internal or external RAID 5 or RAID 6 systems and manual/automatic DVD solutions. Rest assured that you will never run out of storage space, regardless of future policy changes. As storage requirements grow, the only cost would be for addition hard drives or DVDs.

COMMAND CENTER

powered by COBAN

EVIDENCE MANAGEMENT

Take control of with Command Center.

Command Center is COBAN's latest video management system designed specifically for law enforcement agencies. It allows you to manage in-car, body-worn, and interview room videos, as well as, users, and devices, using our intuitive powerful system. Developed with web technologies, Command Center offers users a familiar, internet-like environment.

You make the rules, Command Center does the rest.

Command Center is a rule-based system that automates on-going maintenance. Once you've defined security policies and evidence retention criteria, the system runs by itself. System administrators can spend their time on more productive tasks than routine system maintenance. Rules can be simple or detailed,

Evidence on demand... anywhere, any time.

Command Center is a web-based application that allows authorized users secured access to information from any location with an internet connection. Videos can be exported to your local computer as needed and burning video evidence to DVDs does not require third party software. Everything is at your fingertips.

From car to court, we've got your back.

Command Center hosts and manages videos from in-car systems, body-worn cameras, and interview rooms. The chain of custody is backed-up by an audit trail, every step of the way, to ensure your valuable evidence holds up in court.

Command Center Overview

Full Web interface that is compatible with Cloud, Hybrid, and Local solutions.

Using the same platform and licensing, Command Center can be configured to run from a fully hosted Cloud Solution on the Microsoft Azure Platform, to a locally hosted storage, and even a hybrid solution in between. This allows you to utilize existing infrastructure, as well as "grow into" the cloud gradually. Avoid astronomic hidden fees when migrating large amounts of data in or out of the cloud by utilizing a hybrid approach. Utilize Hybrid to build an automatic data backup in the cloud for a fraction of the cost and complexity of competing replication solutions.

Unified platform for all you Evidence needs

Command Center multiple Coban Video Platforms, including Body Cameras, In-car video systems, Interview Rooms, and Evidence Management. Save time and money on training by using one platform.

Keep up to date using the latest Maps

Powerful Mapping, tracking, and reporting functions powered by Microsoft Bing. Always have the latest Geo-information without worrying about updates or outdated maps.

Template and role based permissions

Never worry about having to manage users individually. Easily create a group that automatically assigns all rights and permissions to users.

Advanced Data mining and integration

Using standard tools, like Microsoft SQL (and its reporting capability) generate reports to help manage your systems and manage everyday tasks.

CAD integration

Ask about how we can integrate your CAD system to automatically assign Case numbers, incident categories, and subject information. If you are able to provide us with a data output from your CAD system, we will integrate free of charge.

Be confident you are covered by Microsoft's CJIS-compliant Cloud solution

If using cloud, rest assured that you data is stored in multiple geographic locations, all housed within the United States, and available with 99.999% uptime.

VIDEO MANAGEMENT: OUR FOCUS, OUR STRENGTH

With more than 14 years of experience developing video management solutions for law enforcement, COBAN knows what matters to you. Command Center is the latest management software from COBAN that benefits from our experience as the leading video management software provider in this industry.

COBAN Technologies, Inc.
11375 West Sam Houston Parkway South #800
Houston, Texas 77031
1 (866) 81-COBAN | 1 (866) 812-6226
www.cobantech.com

Digital Property Manager

Powered by COBAN

OTHER FEATURES

- Supports various types of files such as: video, audio, images, and digital documents (PDF, Word, etc.)
- Users can check files in and out for analysis. The system maintains all versions of the file and complete chain of custody.
- A digital signature is assigned to each file and version.
- Case packages are exported in a data format so the files can be displayed on a computer.
- Users can choose between list view and thumbnail view on file list screen.
- Advanced search function provides a way to search files across all incidents.

Fully Integrated with Coban's Digital Video Management System (DVMS)

Imports all digital media (videos, audio, photos, documents) related to an incident, and catalogs them in a logical way for presentation.

Integrates with Coban's DVMS defined user privileges and system security.

Automatically link Coban in-car and interview room videos with the same incident number for playback and export.

Easily export "case package" to CD/DVD disc, with the option to include metadata and audit trail.

All files are stored and managed by DVMS advanced storage solutions, which include auto-DVD burner and automated tape libraries.

The life cycle of evidentiary files are managed according to the DVMS system policies defined by the administrator.

11375 West Sam Houston Parkway South # 800
Houston, Texas 77031

SECTION 5

Sample Scope of Work

Key Personnel Resumes

COBAN Business Continuity Plan (Disaster Recovery)

Cloud Standard Terms and Conditions

Microsoft Azure Government Security Documents

COBAN Warranty and Support Statements

11375 West Sam Houston Parkway South # 800
Houston, Texas 77031

ALLAN CHEN

EXECUTIVE VICE-PRESIDENT of TECHNOLOGY

Overview

Allan Chen brings solid and progressive experience in all facets of software application development, deployment, project management and business strategy.

Experience

COBAN TECHNOLOGIES – Houston, TX **2002 – Current**

- Design and oversee software development for digital video and mobile date computer applications.
- Software development.
- Project management for customized applications.
- Planning and scheduling.
- Product and strategic planning.
- Broad technology base.
- Strong leadership and management skills.
- Process improvement and change management.
- Human performance, coaching and mentoring.
- Budget and multi-site management.
- Continuous organization improvement.
- Daily operations management.

Education

Master of Science Degree: Computer Science **1986 - 1988**
Lamar University – Beaumont, TX
Subjects: Organizational management, business communications, leadership and supervision, project management, human resources management, critical analysis, interpersonal relations, and office and computer systems.

Projects

Kansas City Police Department

- 354 In-car Video units deployed
- Customized software design
- Multi-site enterprise solution
  - Tape Library
  - Removable Media Transfer
  - Auto DVD Burner

Chicago Police Department

- 1000+ In-car Video units deployed
- Solution presentation
- User training
- Customized software design
- Multi-site enterprise solution
  - Wired and wireless transfer
  - Auto DVD Burner

11375 West Sam Houston Parkway South # 800
Houston, Texas 77031

CINDY CHANG

NATIONAL SALES SUPPORT MANAGER

Overview

As national sales support manager, Cindy Chang is responsible for ensuring all projects have the appropriate resources and support to be executed in a responsive, efficient manner. Cindy oversees the management of physical assets, participates in staff development, and growth strategies. She is also responsible for the continued development and compliance of purchasing and procurement procedures.

Experience

COBAN TECHNOLOGIES – Houston, TX **2003 – Current**

- Responsible for the coordinated management of multiple strategic business projects and organizational objectives.
- Client and vendor relations; build credibility, establish rapport, and maintain communication with internal and external stakeholders.
- Define and initiate projects and assign project managers to oversee cost, schedule, and performance.
- Maintain continuous alignment of program scope with strategic business objectives, and make recommendations to modify the program to enhance effectiveness.
- Periodic dashboard reports on the current program.
- Deliver and execute project deliverables.
- Quality assurance and change control.
- Procurement and outsourcing, dealer recruiting, and continuous process improvement.
- Full life cycle project management.

Education

Bachelor of Business Administration: Accounting **2006**
University of Houston – Houston, TX

Project Management Certificate: **1996**
Project Management Institute

11375 West Sam Houston Parkway South # 800
Houston, Texas 77031

Projects

Los Angeles Police Department
- 1000+ In-car Video units deployed
- Solution presentation
- Test plan design and implementation
- Multi-site enterprise solution
    - Tape Library
    - Disaster Recovery
    - Wired and wireless transfer
    - Auto DVD Burner
- On Going

Chicago Police Department
- 1000+ In-car Video units deployed
- Solution presentation
- User training
- Customized software design
- Multi-site enterprise solution
    - Wired and wireless transfer
    - Auto DVD Burner
- On Going

Washington State Police
- 750+ In-car Video units deployed
- Solution presentation
- Multi-site enterprise solution
    - Disk Raid
    - Removable Media Transfer
    - Wired and wireless transfer
    - DVD Burner
- On Going

San Antonio Police Department
- 650+ In-car Video units deployed
- Solution presentation
- Test plan design and implementation
- Multi-site enterprise solution
    - Virtual Environment
    - Disaster Recovery
    - Wired and wireless transfer
    - Auto DVD Burner
- May 2013

San Antonio Intl. Airport Police
- 65+ Body worn camera units deployed
- Solution presentation
- Test plan design and implementation
- Multi-site enterprise solution
    - Wired and wireless transfer
- March 2015

11375 West Sam Houston Parkway South # 800
Houston, Texas 77031

JERRY CHANG

PRODUCT MANAGER

Overview

As the product manager, Jerry Chang has over eleven years of In-car Video experience and has worked with over 75 law enforcement agencies.

Experience

COBAN TECHNOLOGIES – Houston, TX **2004 – Current**

- Network security and firewalls.
- Enterprise deployment of digital In-car video management.
- End-user training in operations of video systems.
- Administrator training in troubleshooting, management, and policy.
- Microsoft Windows Server, 2005, 2008.
- Microsoft SQL Server 2005, 2008.
- Proxim ORiNOCO products and management.
- Integration with CAD, LPR, and other applications.
- Cohabitating and interfacing with radar, communications, GPS, and mesh networks.
- Backend/infrastructure setup, configuration, and maintenance.
- Develop and execute test plans to improve perception of system and meet project milestones.
- Demonstrate end-to-end system functionality to key personnel, including chiefs and city council members.
- Integrate with existing projects including Northrop Grumman Command Point (computer-aided-dispatch) and Netmotion (communications).
- Provide consulting and recommendations for current and future projects improvements/developments.

Education

Certificate: **Microsoft and CISCO**
Subjects: MCITP, MCSA, MCTS-Enterprise, Windows 2008 and Windows Administration, CCNP, and CCNA

11375 West Sam Houston Parkway South # 800
Houston, Texas 77031

Projects

Kansas City Police Department
- 354 In-car Video units deployed
- Customized software design
- Multi-site enterprise solution
  - Tape Library
  - Removable Media Transfer
  - Auto DVD Burner
- December 2004

Delaware State Police
- 400+ In-car Video units deployed
- Solution presentation
- Multi-site enterprise solution
  - Disk Raid
  - Disaster Recovery
  - Removable Media Transfer
  - Wired and wireless transfer
  - DVD Burner
- May 2015

Corpus Christi Police Department
- 333 Body worn camera units deployed
- Solution presentation
- Test plan design and implementation
- Multi-site enterprise solution
  - Wired and wireless transfer
- March 2014

Los Angeles Police Department
- 1000+ In-car Video units deployed
- Solution presentation
- Test plan design and implementation
- Multi-site enterprise solution
  - Tape Library
  - Disaster Recovery
  - Wired and wireless transfer
  - Auto DVD Burner
- On Going

San Antonio Police Department
- 650+ In-car Video units deployed
- Solution presentation
- Test plan design and implementation
- Multi-site enterprise solution
  - Virtual Environment
  - Disaster Recovery
  - Wired and wireless transfer
  - Auto DVD Burner
- May 2013

11375 West Sam Houston Parkway South # 800
Houston, Texas 77031

DAN LAM

TECHNICAL SUPPORT MANAGER

Overview

As the technical support manager, Dan Lam is a key member of the services division at COBAN Technologies, Inc. He is responsible for motivating the team of technical support associates and for facilitating resolution on escalated calls.

Experience

COBAN TECHNOLOGIES – Houston, TX **2006 – Current**

- Motivate the technical support consultants through performance couching, career planning, and setting educational objectives.
- Participate in quality calibration and validation sessions.
- Improve productivity, recommend changes and conduct training.
- Ensure customer satisfaction and issue resolution.
- Test In-car and Back-end software.
- Write and maintain version documents and software manuals.
- Level III technical support on software.
- Assist in project deployment.

HEWLETT PACKARD (COMPAQ) – Houston, TX **1998 - 2006**

- Provided server deployment solutions that facilitated the installation, configuration, and deployment of high volumes of servers.
- Issue resolution and management.

Education

Bachelor of Business Administration: Management and Finance **1996**
University of Houston – Houston, TX

Certificate: ACT Compaq/HP Hardware

11375 West Sam Houston Parkway South # 800
Houston, Texas 77031

Projects

Chicago Police Department

- 1000+ In-car Video units deployed
- Solution presentation
- User training
- Customized software design
- Multi-site enterprise solution
    - Wired and wireless transfer
    - Auto DVD Burner
- On Going

Ocala Police Department

- 135 Body worn camera units deployed
- Solution presentation
- Test plan design and implementation
- Multi-site enterprise solution
    - Wired and wireless transfer
- September 2014

Kansas City Police Department

- 354 In-car Video units deployed
- Customized software design
- Multi-site enterprise solution
    - Tape Library
    - Removable Media Transfer
    - Auto DVD Burner
- December 2004

11375 West Sam Houston Parkway South # 800
Houston, Texas 77031

LARRY MARR

NATIONAL TECHNICAL SALES SUPPORT

Overview

As national technical sales support, Larry Marr is responsible for reviewing, completing, and negotiating any and all bids and contracts for submission as well as supporting the nationwide network of regional sales managers and their territories. Larry has over 20 years of expertise in technical sales and solution designs.

Experience

COBAN TECHNOLOGIES – Houston, TX **2003 – Current**

- Develop and conduct training courses on the DICVS and storage solutions to new sales representatives and channel partners.
- Assist in the contract negotiation and deployment of DICVS, storage solutions, and upload solutions for projects ranging in size from $50,000 to multimillion/multi-phase projects.
- Assist internal sales reps and channel account partners with the technical sales portion of their projects.
- Establish and maintain partnerships with wireless networking providers.
- Coordinate and review all wireless site survey projects and recommend product solutions based on findings.
- Assist R&D department in developing new product offerings and software modifications.
- Responsible for responding to various RFPs, RFIs, or IFBs for entire internal sales staff and assisting channel partners with their responses.

Education

Certificate: **MCSE, CompTIA**
Subjects: Administrating Windows NT Server 4.0, implementing and supporting Windows NT Server 4.0 (MCSE), TCP/IP, Network Essentials, NT Server 4.0 Enterprise (MCSE), Net + (CompTIA), A+ (CompTIA), Microsoft Office 2000/2003/2008, Windows 2000/2003/2008 Server, IBM, Dell, Compaq, HP platforms.

Projects

Tallahassee Police Department

- 90+ In-car Video units deployed
- Interview Room solution
- Officer-worn camera solution
- Removable media
- Wired and wireless transfer

New Mexico State Police Department

- 300+ In-car Video units deployed.
- Multi-site enterprise solution
- Interview room solution
- Wireless transfer

11375 West Sam Houston Parkway South # 800
Houston, Texas 77031

COBAN Business Continuity Plan

The main objective of the COBAN Technologies Business Continuity Plan is to ensure minimal disruption to services and product delivery in the case of a natural disaster or times of crisis. Natural disasters or times of crisis would involve, but is not limited to, the major loss of a significant number of personnel, the physical structure COBAN is located, technology related to customers and operations, or an extended period of time without building utilities. The following list will highlight the primary responsibilities and actions of COBAN departments and employees in response to such catastrophic events.

Unless otherwise noted, this plan does not address temporary interruptions of duration less than the time frames determined to be critical to business operations.

1. Ability to maintain communications and remote support services for the customer, including notification of disaster occurrence.

2. Ensuring operation critical personnel will be able to perform assigned duties and tasks.

3. Essential data backup and recovery, in regards to both electronic and physical records of importance to the company and customers.

4. Product order and contract fulfillment, including entry, execution, delivery, and billing.

5. Minimizing the effect, long and short term, upon established service, products, and deliverables quality standards.

6. Financial solvency pertaining to the ability to continue services and carry existing contracts to term.

The proceeding information will go into detail about the steps that will be taken to complete the previously listed objectives.

SECTION A – Assigned Personnel Roles and Responsibilities

Business Continuity Management Team

1. Function – To oversee the development, maintenance and testing of recovery plans addressing all essential business functions. In the event of a "disaster" to manage the backup and recovery efforts and facilitate the support for key business functions and restoration of normal activities.

2. Organization – The BCMT is co-chaired by the COBAN Chief Executive Officer and Human Resources Manager, who will serve in the absence of the Chief Executive Officer. The Team is composed of key management personnel and management from each of the areas involved in the recovery process.

3. Interfaces – The team interfaces with and is responsible for all business continuity plans and planning personnel at COBAN.

<u>Preparation Requirements</u>

- Call annual review meeting to go over existing plans and decide needed modifications based on infrastructure change.
- Conduct annual emergency exercise with IT and Customer Support before annual review.
- Maintain proper channel in communicating with employees, such as a social media group.
- Enable a function in CM for employees to update personal phone, email address, and emergency contact info.
- Set policy for critical software utilities storage in shared network drives
- Keep updated employee contact information
- Create emergency communication channel utilizing social media apps
- Annual natural disaster recovery training for employees
- Generate and maintain a list of critical equipment
- Review insurance policy and coverage periodically

Damage Assessment/Salvage Team

1. Function – To report to the Business Continuity Management Team, within two to four hours after access to the facility is permitted, on the extent of the damage to the affected site, and to make recommendations to the BCMT regarding possible reactivation and/or reactivation and/or relocation of user operations.

2. Organization – The Damage Assessment/Salvage Team is headed by the Executive Vice President of Technology and activated during the initial stage of an emergency. The team reports directly to the Business Continuity Management Team, and evaluates the initial status of the damaged functional area, and estimates the time to reoccupy the facility and ability to salvage the remaining equipment. During an emergency situation, the Executive Vice President of Technology will take operational responsibility for implementation of damage assessment. This team draws members from the IT department, Operations department, Customer Service department, Accounting department, Project Manager department, and Engineering department. Following assessment, the team is responsible for salvaging equipment, data, and supplies following a disaster; identifying which resources remain and determining their future utilization in rebuilding the data center and recovery from the disaster.

3. Interfaces – The Damage Assessment/Salvage Team will interface with COBAN's CEO and other ranking Vice Presidents to keep abreast of new equipment, physical structures, and other factors relating to recovery.

<u>Preparation Requirements</u>

- Maintain updated backup of critical information in secured cloud storage. Such information includes company databases, software source code, engineering documentation, business contracts/agreements, etc.
- Coordinate with all departments to establish backup and restore protocols.
- Maintain a VM that hosts COBAN business software, backup the VM to secured cloud.
- Facility / Office Map
- Employee Emergency Contact List
- Damage Assessment/Salvage Team Alternative Contact Information
- Inventory list of telecommunication/computer hardware in the office
- Inventory list of software application used in the office
- Create remote access accounts for all employees
- Forwarding service, which allows incoming calls to be rerouted to pre-determined location or pre-established phone numbers
- Adding a backup ISP and balancing the traffic between the two ISPs over separate communication path
- Damage assessment form
- List of employee contacts

- List of critical computer workstations
- Floor plan with electricity and outlet information
- List of warehouse inventory items
- Items needed to perform assessment such as laptop, flashlights, helmet, gloves, phone, emergency medical kit etc.

To provide appropriate assessment of the IT infrastructure, the damage assessment team will need tools to navigate the building in the aftermath of a disaster such as a flashlight or protective gear, depending on the severity of any possible structural damage to the building. The assessment team will need to review the state of the IT hardware in the server room and each work area. In order to do this, they will need an inventory list of all hardware to do a head count and physical assessment of each piece of hardware. The team will also need documents on critical systems including startup procedures and who for support on said systems. They will also need a list of contacts for services including utilities, E-mail, Internet/Telephone, HVAC, and generator service.

COBAN Public Information Team

1. Function – Public relations planning is required so that when an emergency arises, inquiries from customers, friends and relatives of staff, and media can be handled effectively. The Public Information team is responsible in making sure facts are presented to the involved parties in an accurate, focused, and timely manner.

2. Organization – The team will consist of the Vice President of Sales and Marketing and the Vice President of Major Accounts. In their absence, responsibility will revert to the most senior manager on the scene.

3. Interfaces – The Vice President of Major Accounts and Marketing will interface between COBAN and outside entities. Copies of all status reports generated will be forwarded to the Vice President of Major Accounts and Marketing for potential value in information distribution. He will work in conjunction with the HR department in dissemination of information to staff.

<u>Preparation Requirements</u>

- Maintain a list of external contacts
- Maintain a number of prepared documents that can address potential situations
- Keep an updated emailing list group

COBAN Insurance Team

1. Function – To provide for all facets of insurance coverage before and after a disaster and to ensure that the recovery action is taken in such a way as to assure a prompt and fair recovery from our insurance carriers.

2. Organization – This team will consist of the Chief Financial Officer and Accounting personnel. The team reports through the Business Continuity Management Team; of which it is a member.

3. Interfaces – The Insurance Team will interface with the following teams, relative to insurance matters:
   Damage Assessment/Salvage Team
   Public Information Team

Preparation Requirements

- Ensure insurance policies are sufficient to cover all potential liabilities.
- Keep electronic and physical copies of data and records at an off-site location.

COBAN Telecommunications Team

1. Function – To provide voice and data communications to support critical functions. Restores damaged lines and equipment.

2. Organizations – The team will consist of appropriate IT and Engineering staff. The Telecommunications Team will also coordinate with and supervise outside contractors as necessary. The team will report through the Vice President of Engineering.

3. Interfaces – The Telecommunications Team will interface with the following teams, relative to telecommunications requirements:
   Damage Assessment/Salvage Team
   Public Information Team

Preparation Requirements

- Keep an up-to-date building utilities provider contact list

SECTION B – Notification Procedures

The proceeding personnel/entities should be notified that a natural disaster/crisis event has occurred. All parties involved should be notified before any other action is taken. Dependent upon the severity of the event, the order of listing may or may not hold significance, and some communications may happen concurrently:

Business Continuity Management Team

Damage Assessment/Salvage Team

Telecommunications Team

COBAN Personnel and Employees not directly involved in the BCP process, in addition to families if necessary.

Public Information Team

Insurance Team

All customers potentially affected by the disruption in COBAN standard business operations

Any affected or involved outside entities (contractors, clean-up crews, etc)

SECTION C – Actions and Procedures Taken by the Business Continuity Plan Teams in Response to an Event

Business Continuity Management Team Coordination

This subsection contains instructions to the Business Continuity Management Team regarding coordination of the COBAN disaster/crisis response.

Action Procedures:

Main Coordinator ensures entire Business Continuity Management Team (BCMT) has been notified.

Notify appropriate staff to meet at a previously designated safe, off-site location.

Main coordinator to Meet with Damage Assessment Team to review their findings and present results to BCMT.

Main coordinator to present recommendations to BCMT for next steps in recovery effort.

Main coordinator to begin notification of all recovery teams. Check to ensure all recovery participants have been notified.

Main Coordinator to monitor the activities of the recovery teams. Assist them as required in their recovery efforts.

Main coordinator to report to other BCMT members on a regular basis on the status of recovery activities.

Main coordinator, on an hourly basis, or other appropriate interval, update the Recovery Status information message via email, website update, or telecommunications.

Damage Assessment

This subsection contains instructions to the Damage Assessment/Salvage Team for initial disaster response and recovery efforts.

Action Procedures:

Notify team members and/or appropriate contractors to report to the site for initial damage assessment and clean-up. Communication should be through two other channels in addition to company email, such as social media, cell phone, home phone, and personal email.

Conduct briefing regarding the anticipated primary areas of damages.

Coordinate transportation and supplies.

Ensure that all electronic power supplies are cut to any area equipment that could possess a threat to personal safety.

Ensure that under no circumstances is power to be restored to computer equipment until the comprehensive damage assessment has been conducted, reviewed, and authority to restore power has been expressly given by the BCMT.

Issue work orders and call appropriate personnel.

Team Leader Request permission to enter site from Fire Department (if required).

Take a service representative from each of the appropriate vendors, the insurance claims representative and appropriate Physical Plant and Information Systems personnel into the site.

Team Members Review and assess the damage to the facility. List all equipment and the extent of damage. List damage to all support systems (power, A/C, fire suppression, communications, etc.).

Photograph all damaged areas as soon as possible for potential insurance claims.

Team Leader Notify the BCMT as to the severity of the damage and what can potentially be salvaged.

Team Leader Notify the BCMT if the area be restored to the required level of operational capability in the required time frame.

Issues to consider:

- Origin of the emergency or disruption
- Potential for additional disruptions or damage
- Area affected by the emergency
- Status of physical infrastructure
- Inventory and functional status of the most important equipment

- Type of damage to equipment
- Items to be replaced
- Estimated time to restore normal services if disaster procedures were not in place

Activation Planning

This subsection contains instructions to the Business Continuity Management and Damage Assessment/Salvage Teams in regards to considerations that should be given in order to determine an appropriate response.

List of systems and services that need to be restored

- Conduct briefing regarding the anticipated primary areas of damages
- Coordinate transportation and supplies
- Ensure that all electronic power supplies are cut to any area equipment that could possess a threat to personal safety
- Ensure that under no circumstances is power to be restored to computer equipment until the comprehensive damage assessment has been conducted, reviewed, and authority to restore power has been expressly given by the BCMT
- Critical systems such as VM that runs corporate business software and databases
- Corporate file system and contents (including business documents and software/engineering source code)
- Customer support communications
- Operations critical workstations will need to be reestablished

Their interdependencies and sequence of restoration

- Operations critical workstations will need to be restored
- Corporate software and databases
- Shared network drives
- Customer services

Time estimations for each restoration (will documented in detail)

Instructions for reporting failures to the team leads

Plan for communication between teams

The damage assessment team will compile a list of systems and services that need to be restored. These items will be prioritized based on the critical needs of the business and how quickly they can be restored. The interdependency of certain systems and services will dictate the priority and may

promote the item to a higher priority level. If a critical system cannot operate properly without another system, that system will be considered critical, even if assessed individually to not be a critical system. An example would be setting up a client workstation so that the data from CM can be accessed. Some items with a lower priority may be restored before more critical items if they have a short recovery time and resources are not being used to restore more critical items. In the event that this happens and a more critical item needs these resources, the restoration of these lower priority items will be suspended until the resources become available or the item becomes the highest priority. Using the data collected from previous assessment of these systems, the assessment team will determine a reasonable estimation to restore each service.

The team will provide to the department leads a flash report every 4 hours as needed of the damage assessment, a more complete report of the failure assessment will be provided daily.

The flash report will include

- systems that are damaged,
- the severity of the damage,
- the expected time to restore
- Any previously reported systems that have been restored

The daily report will include a comprehensive list of all damaged systems included in previous reports along with a more detailed plan of recovery if needed.

Communication between team members and department leads will handled through phone calls, and text communication using E-mail. When appropriate, or when e-mail is unavailable, alternate means of text communication will be handled using phones or a messaging app like Line.

Salvage Operations, Sequence of Recovery Activities and Procedures

This subsection contains instructions to the Damage Assessment/Salvage Team regarding salvage operations and what actions should be taken to begin the recovery process.

Team Leader have all necessary members of any Team report to the Staging Area. If the business location is not accessible or in a condition deemed to be unusable, a staging area would be one of company executives' residency. Note that mobile generators might be needed to sustain temporary operation.

Prior to performing any salvage operation contact Insurance Team to coordinate with possible insurance claims requirements and appraisals.

Have the staff and/or appropriate contractors start salvaging any furniture and equipment.

Gather vital records and other materials that were retrieved from the primary site and determine appropriate storage locations

Determine which vital records, forms, and supplies are missing.

Based upon advice from Insurance Team and customer engineering, contact appropriate vendors regarding reconditioning of damaged equipment

Team Leader Meet with the Business Continuity Management Team Coordinator to provide status on salvage operations.

Issues to consider:

- Get authorization to access damaged premises or geographic area
- Notify users associated with the system
- Obtain required office supplies and work space
- Obtain and load backup media
- Restore critical operation procedures

Public Information Dissemination

This subsection contains the actions that should be taken by the Public Information Team.

Public Information Team Lead assesses the scope of the emergency, in consultation with senior management if necessary, and determine the appropriate public relations course of action.

In instances where media are notified immediately, due to fire department or police involvement, the Public Information Team Lead will proceed to the scene at once to gather initial facts. Emphasis must be placed upon getting pertinent information to the employees and customers as quickly as possible.

Member of the Public Information Team will maintain a log of all incoming calls to ensure a quick response to media and other requests.

Member of the Public Information Team will maintain a log of all information which has been released to the media.

Public Information Team Lead, when appropriate, will prepare information releases on a periodic basis for distribution to the affected customers and COBAN employees.

If employee injuries or fatalities are involved, notify appropriate family members and management personnel.

Public Information Team Lead should be aware as soon as families have been informed. This will permit the release of names and addresses of victims so that families of those not involved can be relieved of anxiety.

Public Information Team Lead will contact the public relations director(s) at the hospitals where injured have been taken to coordinate the release of information.

In cases where long-term media coverage is anticipated, establish a Press Room in the (location to be selected) Provide for telephone requirements of the press.

If media wants to photograph physical damage, clear the request with local Police prior to approving request. Then accompany all photographers.

Public Information Teams will coordinate information releases after the immediate emergency has passed.

Insurance Considerations

This subsection will outline the actions and areas of concern for the Insurance Team.

Insurance Team Leader will contact the appropriate Insurance people upon first advice of disaster.

Insurance Team Leader will meet with Damage Assessment/Salvage team at site.

Insurance Team Leader will go through the disaster scene with Damage Assessment/Salvage team and advise on matters relating to insurance and claims. He will ensure that nothing is done to compromise recovery from insurance carrier and photograph all applicable areas.

Insurance Team Leader will file all appropriate claims forms with all involved insurance carriers.

The Insurance Team will report status of claims activity to the Business Continuity Management Team.

Telecommunications Restoration

This subsection pertains to the duties and actions to be taken by the Telecommunications Team.

Telecommunications Team will oversee the assessment of damage to telecommunications facilities. Directs contingency and recovery efforts. Provides updates to Business Continuity Management Team and appropriate COBAN management.

Telecommunications Team will work with the operations and customer service manager to arrange for voice and dial-up data communications services to support critical functions. Procures stock to repair or replace damaged equipment. Restores full services in a timely manner.

Telecommunications Team will provide data communications facilities or circuits to support critical functions. Assists with restoration of cable and wire plant, as needed. Assists Information Systems and other departments with relocation and restoration of data facilities.

SECTION D – Services and Operations Priority

This section will outline the priorities of each COBAN department in regards to essential services and operations. This will assist each department in restoring the operations that will most affect the delivery of goods and services to the customer.

Engineering/IT

In preparation of a disaster, the strategy chosen is to back up all critical software systems and data and store the backup media off-site. This strategy entails the procedure for maintaining off-site storage of critical data to be restored to new/recovered hardware acquired after a disaster.

High Priority:

- Server and Pertinent Data Backup. Key business processes and the agreed backup strategy for each will be listed in the following table. The strategy chosen is off-site data storage (OSDS), which entails maintaining off-site storage of critical data to be restored to new or recovered hardware acquired after a disaster. This includes systems and servers, critical data stored in file shares, network/firewall configuration, and business operations databases.
- Networking and communications for the physical building
- Electronic Data security
- Business operations software functionality

Customer Service/Tech Support

High Priority:

- Available personnel to address customer support calls
- On site (travelling) personnel still have access to the tools needed (HQ support)
- Maintain ability to perform most common support tasks

Sales and Marketing

High Priority:

- Communications with external entities (press release, media coverage)
- Situational updates to employees
- Communicate with customers regarding the disaster and re-solicit phone contacts
- Acquire needed vital documents
- Access missing documents and files and reconstruct, if necessary

- A contingency method to take or execute work orders
- Appointments with customers will be kept if possible, but if not, ample warning will be given and rescheduled at an agreed upon time
- Regional Sales Managers will still have access to the tools and support needed

Project Management

High Priority:

- Establish remote offices
- Account obligations will be maintained to the best of ability
- Communicate with customers regarding the disaster and re-solicit phone contacts
- Acquire needed vital documents
- Access missing documents and files and reconstruct, if necessary
- Set up operation
- If any disruptions will affect accounts, the customer must be notified immediately

Hardware, Inventory, and Shipping

High Priority:

- Available emergency inventory of necessary products and office tools is maintained. This entails requesting the vendor to stock long lead-time parts, keeping a portion of emergency inventory at an off-site location, and maintaining a list of needed office tools.
- Storage and maintenance of inventory is as resistant to a crisis situation as reasonably possible. To accomplish this, inventory items will be stocked on pallets or carts with wheels to ensure quick transportation in the event of an emergency. Also, safety equipment, such as smoke detectors, monitoring devices, and fire extinguishers will need to be kept in good condition and periodically checked. Exits and entrances to the warehouse need to be clear from obstructions. In addition, flammable or delicate storage materials usage should be at a minimum. A maintenance crew should inspect the building's roof regularly.
- Work order fulfillment and product obligations to customers. Work order information and software will be duplicated to a remote server on a regular basis. Critical software utility tools must also be located on the network shared drives.
- Delivery service, both incoming and outgoing, will resume when safe and as soon as possible. This will be achieved by contacting the parcel service companies to request temporary package forwarding if necessary.
- Product and hardware repairs critical to the customer are still being carried out. RMA safety stock will be maintained at an off-site location.

- Preservation of reasonable, agreed upon quality standards of goods sent to the customer. A simplified QA inspection procedure focuses on key system functionality and reduce overall inspection time.

Accounting and HR

High Priority:

- Financial records, both for COBAN and the customer, are duplicated and kept safe
- Proper company insurance is maintained
- Minimum safety standards for the work environment are established and reviewed
- Sensitive customer data will be kept secure
- Sensitive employee data will be kept secure
- Employees are well aware of the Business Continuity Plan and any updates/changes to the policy
- In situations where employees are the most affected by an event, how the company will compensate and assist them so they may return to work, if possible.

TERMS & CONDITIONS

COMMAND™ TERMS OF USE

This is an agreement (the “Agreement") between you and COBAN Technologies, Inc. (with its affiliates, "COBAN", "we" or "us") regarding the Command™ service and associated software (the "Service"). Before using the Service, please read these Terms of Use, all rules and policies related to the Service. If you use the Service, you will be bound by the Agreement. It is effective on the date we provide you with confirmation of your Subscription or the date on which your Subscription is renewed as applicable.

1. THE SERVICE

1.1. THE SERVICE. The Service provides storage, retrieval, management and access features and functionality for your data ("Your Files"). By using the Service, you are directing us to store, manage, and provide access to Your Files on your behalf.

1.2. USING YOUR FILES WITH THE SERVICE. You may use the Service only to store, retrieve, manage, and access Your Files using the features and functionality we make available. You may not use the Service to store, transfer or distribute content of or on behalf of third parties, to operate your own file storage application or service, to operate other commercial service, or to resell any part of the Service. You are solely responsible for Your Files and for complying with all applicable copyright and other laws, including import and export control laws and regulations, and with the terms of any licenses or agreements to which you are bound. You must ensure that Your Files are free from any malware, viruses, Trojan horses, spyware, worms, or other malicious or harmful code. You may not reverse engineer, decompile, disassemble, or work around technical limitations in the Service, except to the extent that applicable law permits it despite these limitations. You may not disable, tamper with, or otherwise attempt to circumvent any billing mechanism that meters your use of the Service. You may not rent, lease, lend, resell, transfer, or sublicense the Service or any portion thereof to or for third parties.

The Services and data storage are subject to usage limits in the quantities specified in purchase orders. Unless otherwise specified, (a) a quantity in purchase orders refers to end users, and the Service may not be accessed by more than that number of end users, and (b) an end user identification may be reassigned to a new individual replacing one who no longer requires ongoing use of the Service. You and each of your end users agree to adhere to this Agreement and all laws, rules, regulations, and policies applicable to your use of the Services. If you become aware of any violation of this Agreement by an end user, you will immediately terminate that end user’s access to Your Files and the Services.

1.3. SHARING YOUR FILES. The Service may provide features that allow you to share Your Files with others. You may only share Your Files in which you have all necessary rights. If you share a file, anyone with access to that file may view and download copies of the file. You are solely responsible for how you share Your Files and who may access Your Files that you share.

Sharing Your Files is permitted for licensed users and entities directly involved with fair use of Your Files. COBAN reserves the right to restrict access to Your Shared Files if usage exceeds commercially reasonable and appropriate levels, such as excessive usage resulting from distribution of Your Shared files through common logons or public forum.

1.4. QUALIFICATION. To qualify for the Service and COBAN pricing plans, we require a review and approval of (i) the number of professional licenses requested, you’re your data retention policy post-365 days, (iii) your policy regarding FOIA requests, and (iv) shift recording policy.

1.5. END USERS. You control access by End Users, and you are responsible for their use of the Service in accordance with the Term of Use and Terms and Conditions of this agreement.

2. Service Plans

2.1. SERVICE PLANS; TRIAL PLANS. The Service offers plans with different limits and fees (each a "Service Plan"). We may offer trial or promotional Service Plans ("Trial Plans"). Trial Plans may be subject to additional terms.

2.2. FEES. The price stated for each Service Plan does not include any taxes that we may charge. Payment is non-refundable, even if you stop using the Service.

2.3. CHANGING YOUR SERVICE PLAN. If you upgrade your Service Plan, the upgrade will take effect immediately, we will charge you the applicable fee, and your Service Plan term may be extended, as described at the time you upgrade. If you downgrade your Service Plan, unless otherwise specified, the downgrade will take effect at the end of the term of your existing Service Plan. If you no longer have a Service Plan or exceed your Service Plan’s storage limit, including by downgrading or not renewing your Service Plan or no longer qualifying for an Additional Benefit, we may delete or restrict access to Your Files.

3. USE OF THE SERVICE

3.1. USE OF YOUR ACCOUNT. You may only use your Service Plan in connection with one account. You may not share your username and password with others or use anyone else's username and password. You are responsible for maintaining appropriate security and protection of Your Files.

3.2. USAGE RESTRICTIONS AND LIMITS. The Service is offered in the United States. There may be limits on the types of content you can store and share using the Service, such as file types we don't support, and on the number or type of devices you can use to access the Service. We may impose other restrictions on use of the Service. We do not support any full-shift recording policies. The Service requires you to periodically delete closed cases files from Command™ Cloud service.

3.3. OUR USE OF YOUR FILES TO PROVIDE THE SERVICE. We may use, access, and retain Your Files in order to provide the Service to you and enforce the terms of the Agreement, and you give us all permissions we need to do so. These permissions include, for example, the rights to copy Your Files for backup purposes, modify Your Files to enable access in different formats, use information about Your Files to organize them on your behalf, and access Your Files to provide technical support.

3.4. PRIVACY AND DATA LOCATION. We will control the location of your storage and the right to utilize other method of Cloud storage for data held past the retention period.

We treat Customer Data in accordance with our Privacy Statement. Subject to any restrictions set forth in the Privacy Statement, we may transfer to, store, or process Customer Data in any country where we or our Affiliates or subcontractors have facilities used to provide or support the Services. We are a data processor (or sub-processor) acting on your behalf, and you appoint us to do these things with Customer Data in order to provide the Services to you. You will obtain any necessary consent from End Users or others whose personal information or other data you will be hosting using the Services.

3.5. OWNERSHIP OF YOUR FILES. Except for Software we license to you, as between the parties, you retain all right, title, and interest in and to Your Files. We acquire no rights in Your Files, other than the right to host data within the Services, including the right to use and reproduce Your Files solely as necessary to provide the Services.

3.6. USE OF YOUR FILES. We will use Your Files only to provide you the Services. This use may include troubleshooting to prevent, find, and fix problems with the operation of the Services. It may also include improving features for finding and protecting against threats to users. We will not use Your Files or derive information from it for any advertising or other commercial purposes without your consent.

3.7. THIRD-PARTY REQUESTS. We will not disclose Your Files to a third party except as you direct or unless required by law. Should a third party contact us with a demand for Your Files, we will attempt to redirect the third party to request that data directly from you. As part of this effort, we may provide your basic contact information to the third party. If compelled to disclose Your Files to a third party, we will promptly notify you and provide a copy of the demand, unless legally prohibited from doing so. You are responsible for responding to requests by third parties regarding your use of the Services.

4. SOFTWARE

4.1. USE OF THE SOFTWARE. We may make available to you software for your use in connection with the Service (the "Software"). Terms contained in the TERMS & CONDITIONS OF SALE apply to your use of the Software.

4.2. INFORMATION PROVIDED TO COBAN. The Service and the Software may provide us with information relating to your use and the performance of the Service and the Software, as well as information regarding the devices on which you download and use the Service and the Software.

5. CHANGES; SUSPENSION AND TERMINATION

5.1. CHANGES. We may change, suspend or discontinue the Service, or any part of it, at any time without notice. If we discontinue the Service, we will give you a prorated refund of any fees paid for your Service Plan based on the number of full months remaining in your Service Plan.

5.2. SUSPENSION AND TERMINATION. Your rights under the Agreement will automatically terminate without notice if you fail to comply with its terms. We may terminate the Agreement or restrict, suspend or terminate your use of the Service at our discretion without notice at any time, including if we determine that (i) your use violates the Agreement, (ii) is improper, substantially exceeds or differs from normal use provided from approved recording and retention policy, statement of work, quotations, or other relevant paperwork, (iii) involves fraud or misuse of the Service or harms our interests or those of another user of the Service, (iv) poses security risks to the Service, (v) delinquent on your payment obligations for more than 90 days, or (vi) You have become the subject of any bankruptcy, reorganization, liquidation, dissolution, or similar proceeding. If your Service Plan is restricted, suspended or terminated, you may be unable to access Your Files and you will not receive any refund of fees or any other compensation.

We have no obligation to maintain or provide any of Your File should you terminate the Service. Requests for additional assistance to you in transferring and retrieving Your File will result in additional fees from us and we will not warranty or guarantee data integrity or readability in the external system.

5.3. IP RIGHTS. We or our licensors own and reserve all right, title, and interest in and to the Command™ Services and related software. Subject to the terms of this Agreement, we grant you a limited, revocable, non-exclusive, non-sublicensable, non-transferrable license to access and use the Command™ Services solely in accordance with this Agreement during the Term. We own all right, title, and interest in and to Command™ Services, including without limitation all Intellectual Property Rights. If you or your end users provide any suggestions to us for enhancements or improvements, we will own all right, title, and interest in and to the suggestions and have the right to use the suggestions without restriction, even if you or your end users have designated the suggestions as confidential. You irrevocably assign to us all right, title, and interest in and to the suggestions and agree to provide us any assistance we may require to document, perfect, and maintain our rights in the suggestions.

TERMS & CONDITIONS

6. GENERAL

6.1. NO WAIVER. Our failure to insist upon or enforce your strict compliance with the Agreement will not constitute a waiver of any of our rights.

6.2. AMENDMENT. We may amend the Agreement at our sole discretion by posting the revised terms in the Service. Your continued use of the Service or the Software after any amendment evidences your agreement to be bound by it.

6.3. CONTACT INFORMATION; COPYRIGHT NOTICES. For communications concerning the Agreement, please write to COBAN Technologies, Inc., Attn: Legal Department, 11375 W. Sam Houston Parkway S. #800, Houston, TX 77031.

6.4. DISPUTES/BINDING ARBITRATION. Any dispute or claim arising from or relating to the Agreement or the Service is subject to the binding arbitration, governing law, disclaimer of warranties and limitation of liability. You agree to those terms by entering into the Agreement or using the Service.

6.5. LIMITATIONS OF LIABILITY. UNLESS LAWS PRESCRIBE OTHERWISE, IN NO EVENT SHALL COBAN OR IT'S AFFILIATES OR VENDORS BE LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF CUSTOMER'S PURCHASE OR USE OF ANY PRODUCT, EVEN IF COBAN, THE AFFILIATE OR VENDOR HAS ADVANCE NOTICE OF THE POSSIBILITY OF SUCH DAMAGES. THE AGGREGATE LIABILITY OF EACH PARTY UNDER THIS AGREEMENT IS LIMITED TO DIRECT DAMAGES UP TO THE AMOUNT PAID UNDER THIS AGREEMENT FOR THE PRODUCT GIVING RISE TO THAT LIABILITY DURING THE 12 MONTHS BEFORE THE LIABILITY AROSE.

6.6. NO THIRD-PARTY BENEFICIARIES. There are no third-party beneficiaries to this agreement.

6.7. WAIVER. The failure of either party to enforce any provision of these Terms shall not be construed as a waiver of such provision or the right thereafter to enforce each and every provision.

6.8. FORCE MAJEURE. Neither party will be liable for any failure in performance due to causes beyond its reasonable control (such as fire, explosion, power blackout, earthquake, flood, severe storms, strike, embargo, labor disputes, acts of civil or military authority, war, terrorism (including cyber terrorism), acts of God, acts or omissions of Internet traffic carriers, actions or omissions of regulatory or governmental bodies (including the passage of laws or regulations or other acts of government that impact the delivery of Services). This section will not, however, apply to Customer's payment obligations under this agreement.

6.9. ASSIGNMENT. Customer may not assign or otherwise transfer its rights or obligations under these Terms without the prior written consent of COBAN, and any attempt to do so shall be void.

6.10. ATTORNEY'S FEES. COBAN shall be entitled to recover its reasonable costs and attorneys' fees, both at trial and on appeal, in any litigation based on these Terms in which COBAN is the prevailing party.

6.11. GOVERNING LAW. The rights and obligations of the parties hereunder shall be governed by and construed in accordance with the laws of the jurisdiction where COBAN is legally constituted, without application of the United Nations Convention on Contracts for the International Sale of Goods.

6.12. ENTIRE AGREEMENT. These Terms and the quotation, acknowledgement, proforma or invoice issued by COBAN to which they are attached comprise the entire agreement between COBAN and Customer and supersede any prior or contemporaneous negotiations or agreements with respect to their subject matter. No amendment shall be effective unless it is in writing and signed by an authorized representative of COBAN and Customer.

Microsoft

Microsoft Azure Government

Overview

Published December 2014

Contents

Executive Summary

In today's dynamic and changing U.S Public Sector environment, many federal, state and local agencies are being asked to find more effective ways to engage with their citizens and to achieve better cross-agency collaboration. At the same time, their IT organizations need to become more agile, minimize datacenter investments, and maximize existing investments by adopting a hybrid cloud approach while still meeting higher levels of security, privacy and compliance requirements. Azure Government is the next step in Microsoft's One Government cloud evolution to help U.S. government organizations meet these challenges.

This paper provides an overview of the Azure Government Cloud capabilities and the trustworthy design and security used to support compliance applicable to federal, state, and local government organizations and their partners.

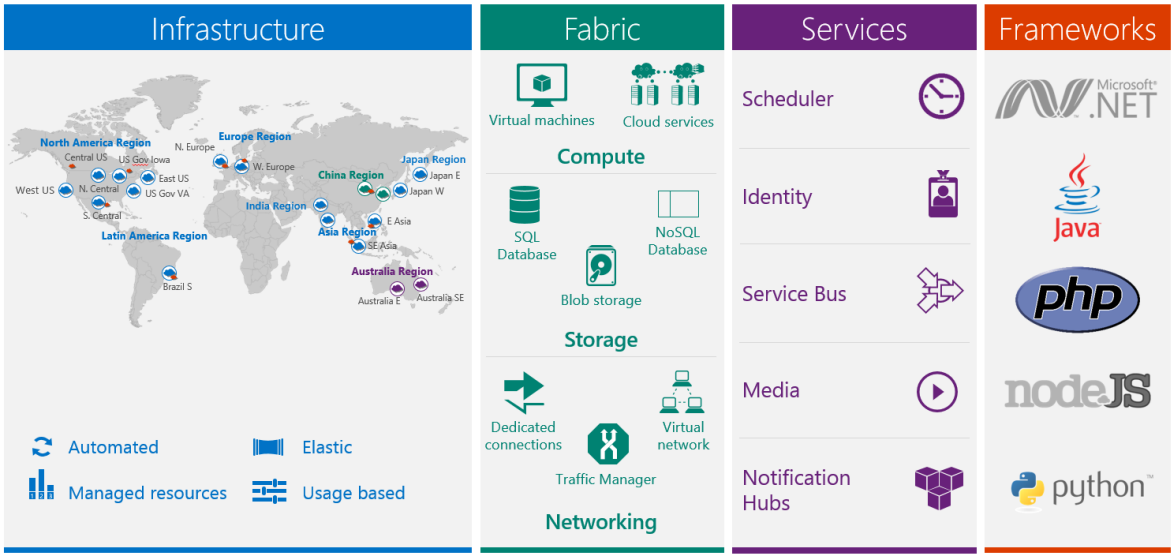
The intended audience for this whitepaper includes:

- U.S. federal, state and local government organizations interested in Enterprise Cloud Services
- Technical decision makers and IT professionals considering Azure for Cloud services.

Azure Government is a *government-community cloud (GCC)* designed to support strategic government scenarios that require speed, scale, security, compliance and economics for U.S. government organizations. It was developed based on Microsoft's extensive experience delivering software, security, compliance, and controls in other Microsoft cloud offerings such as Azure public, Office 365, O365 GCC, Microsoft CRM Online etc.

In addition, Azure Government is designed to meet the higher level security and compliance needs for sensitive, dedicated, U.S. Public Sector workloads found in regulations such as United States Federal Risk and Authorization Management Program (FedRAMP), Department of Defense Enterprise Cloud Service Broker (ECSB), Criminal Justice Information Services (CJIS) Security Policy and Health Insurance Portability and Accountability Act (HIPAA).

Below is a summary view of the Azure Government Cloud infrastructure, fabric, services and frameworks that are available or in preview to help government organizations build hybrid cloud solutions to meet their goals. We will address each of these topics in more detail throughout the rest of the paper. As new services and features are added often, please review the Azure Regions page for specific services.



Azure Government includes the core components of Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS). This includes infrastructure, network, storage, data management, identity management and many other services. Azure Government supports the same great features that public Azure customers have leveraged like Geo-Synchronous data replication and auto scaling. Microsoft has been identified as the leader in both IaaS and PaaS by leading industry analysts.

In addition to providing the robust services and features of public Azure, Azure Government provides a number of features to assure US government entities that their data is secure by providing:

Physical and network-isolated instance – The Azure Government environment is a completely separate instance from Microsoft Azure public and only used by qualified U.S. government organizations and solution providers.

Security, Privacy & Compliance - Microsoft has implemented its robust security, privacy, and compliance controls framework plus additional stringent controls to meet the higher level requirements found in ECSB Impact Levels and CJIS.

Data Storage – The Azure Government environment maintains 2 datacenters over 500 miles apart. All customer managed data is stored within the Continental United States (CONUS) datacenters

U.S. Personnel – All Azure Government operators and administrators are screened U.S.

citizens.

Identity Management – Identity Management within the Azure Government environment is a separate instance of Azure Active Directory.

Compliance – Microsoft is continuously investing to meet and maintain rigorous and changing federal, state, and local compliance requirements such as FedRAMP, CJIS, ECSB, and HIPAA for U.S. government cloud solutions.

Cloud Integration – Azure Government provides an integrated environment with O365 Government allowing for a single sign-on across cloud services and enhanced services such as 1TB of OneDrive storage space.

Azure Government also enables organizations to maintain their existing technology investments and realize the benefits of cloud services. Since Azure Government is an interoperable cloud platform, with products and technologies organizations can build applications that are more open from the ground up. Agencies can choose the tools, services, operating system, architecture, and frameworks including Windows, Linux, Oracle, SharePoint, .NET, Java, PHP and Node.js, for their cloud solutions. The flexibility of the Azure Government platform allows for new forms of cross-agency collaboration, application development, and integration.

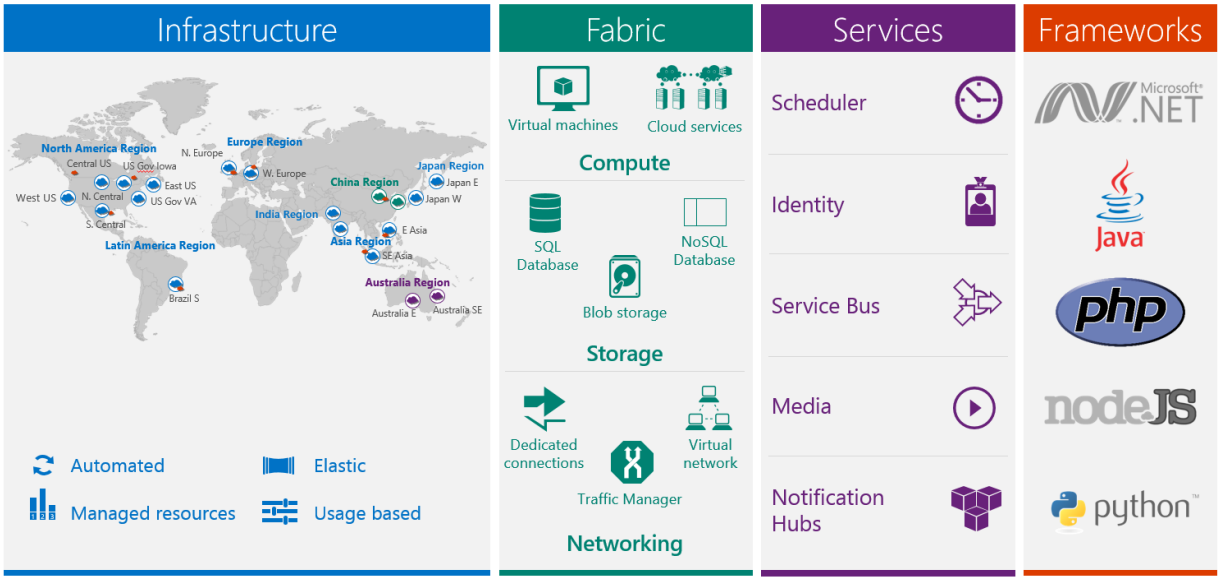
U.S. government organizations interested in cloud services can be confident that Azure Government provides enormous scale and rigorous security practices to meet their evolving needs.

Microsoft Azure Government

Overview

Azure Government delivers a United States based cloud solution designed specifically to support strategic scenarios for U.S. government organizations including the Department of Defense, federal, state, and local governments, and their solution providers. It provides a comprehensive and open Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS) for the U.S. government community including infrastructure, network, storage, data management and identity management delivered through secure and compliant hybrid cloud solution.

Azure Government core components include Compute, Storage, Networking, Identity and SQL database. Below is a diagram depicting the core capabilities that are delivered by Azure Government for IaaS and PaaS and will be discussed in detail below.



Azure Government was designed with the principles outlined below to help government organizations embrace cloud services. The key principles are:

- **Ease of Use** - Make it easy for developers, system administrators, and architects to build, migrate, deploy, and manage applications, and lets you accelerate provisioning of resources to minutes instead of days or months.
- **Open and Flexible** – Empower developers to choose the framework, tools, operating system and architecture to best meet their needs to build cloud solutions including .NET, Java, PHP and Node.js.

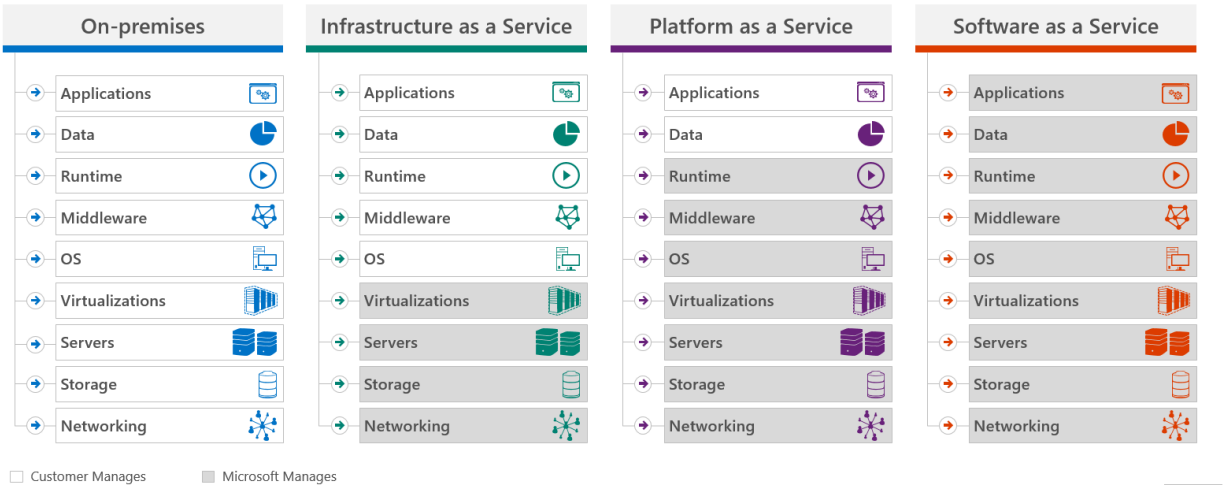
- **Secure and Compliant** – Ensure Azure Government is using Microsoft Azure's world class security, compliance, and controls and is leveraging datacenters in the Continental U.S. (CONUS), screened U.S. personnel and policies to meet the higher level demands of US public sector customers.
- **Enterprise Ready**- Provides enormous scalability, reliability, and use of common management and identity tools that enables hybrid cloud solutions to quickly build, migrate, deploy, and manage, reliable and scalable applications using existing IT environments.

When organizations combine the core Azure Government services above with these principles, it enables them to implement relevant scenarios and capture the benefits of the cloud. In the Azure Government features section, we will break down the core components to help you understand the core services and then discuss some common workloads.

Shared Responsibility

Microsoft believes that security, privacy, and compliance for its government cloud services are a shared responsibility. Microsoft helps reduce the security and compliance burden for its customers by providing trustworthy enterprise cloud services, while also offering the security capabilities and flexibility customers need to use the services in accordance with their own standards.

The following diagram illustrates the shared responsibility approach between an on-premises service managed by the customer and the areas that Microsoft is responsible for in the applicable cloud model.



Microsoft is responsible for the platform and provides cloud services that can meet the security, privacy, and compliance needs of government customers. Customers are responsible for the

environment once the service has been provisioned, including applications, data content, virtual machines, access credentials, and compliance with regulatory requirements applicable to the particular agency.

Trustworthy Design and Operation

Azure Government is built on a Trustworthy Computing foundation consisting of Security, Privacy, and Reliability. Microsoft creates, implements, and continuously improves security-aware software development, operational, and threat mitigation practices, and shares this knowledge with government and commercial organizations. Microsoft engages in industry-leading security efforts through the creation of centers of excellence, including the Microsoft Digital Crimes Unit, Microsoft Cybercrime Center, and Microsoft Malware Protection Center. Key components of Trustworthy Design and Operations include:

- **Software Development Lifecycle (SDL).** Azure development adheres to the Security Development Lifecycle (SDL). The SDL became central to Microsoft's development practices a decade ago and is shared freely with the industry and customers. It embeds security requirements into systems and software through the planning, design, development, and deployment phases including:
- **Rigorous Operations Security Controls.** Azure has developed and adheres to a rigorous set of security controls that govern operations and support. In addition, the Azure team works with other entities within Microsoft such as *Office 365* and the *Microsoft Operational Security Assurance (OSA)* group to identify risks and share information to improve the ability to prevent, detect, contain, and respond to operational security threats both specific to Azure and organization-wide.
- **Assume breach.** The "assume breach" strategy is used to harden Microsoft Government Cloud services. A dedicated "red team" of software security experts simulates real-world attacks at the network, platform, and application layers, testing Azure's ability to detect, protect against, and recover from breaches. By constantly challenging the security capabilities of the service, Microsoft can stay ahead of emerging threats.
- **Incident response.** Azure has a global, 24x7 incident response service that works to mitigate the effects of attacks and malicious activity. The incident response team follows established procedures for incident management, communication, and recovery, and uses discoverable and predictable interfaces internally and to customers.

Microsoft's SDL guidance is also recommended to customers of Azure, since the security of applications hosted on Azure depends on the customers' development processes.

Azure Government Features

Azure Government provides a breadth of capabilities and services including infrastructure, fabric, services, and the frameworks that can be used to develop applications.

Its core capabilities include IaaS and PaaS which provides a rich set of compute, network infrastructure, storage, and identity management services. These provide government organizations the flexibility to choose either approach to quickly build, test, deploy, and manage applications. All government customer data, applications, and hardware reside in the Continental United States (CONUS) and are operated by screened U.S. Citizens.

This section will describe these capabilities in more detail. For further descriptions of Azure Government capabilities refer to the Azure Government Trust Center features and references section.

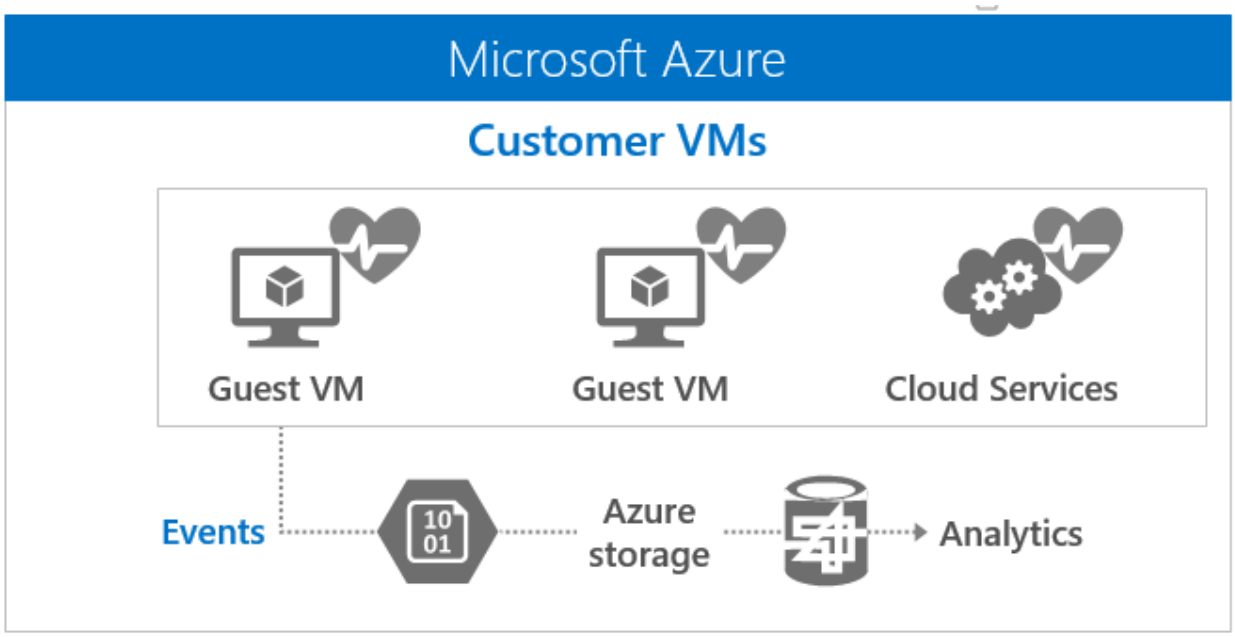
Compute Services

Azure Government compute services can be broken into two classes: *Azure Virtual Machines and Azure Cloud Services*. The primary difference between these offerings is which aspects of routine maintenance are handled automatically by Azure versus which are performed by the customer. The less customization made to the environment, the fewer routine maintenance tasks will need to be performed. Each type of compute service within Azure Government supports auto-scaling to help make sure performance, resource allocation, and cost can be balanced based upon customer objectives.

Azure was designed so that all maintenance of customer services could be done via the portal and Service Management APIs (SMAPI), optionally login accounts can be created on Virtual Machines (VMs) and then connect to the services via either the Remote Desktop Protocol (RDP) or PowerShell. There are also APIs that provide direct access to customer storage accounts and the file systems behind customer Web sites.

Virtual Machines

The Azure Virtual Machines service provides on-demand, scalable computing resources. An Azure virtual machine is a virtual server, hosted on a physical server, in the cloud that the customer configures and maintains according to their needs. It provides the flexibility of virtualization without the expense of buying and maintaining the hardware to host it.



Additionally, Azure virtual machines have the ability to:

- Deploy available versions of Windows Server or several distributions of Linux operating systems by choosing from preconfigured images hosted in the Image Gallery. Or, customer created virtual hard disks (VHD) can be uploaded that contains a server operating system and then used to create virtual machines.
- Create and connect multiple virtual machines so traffic can be load balanced among them.
- Use both automated and manual ways to create, manage, and delete a virtual machine. The web portal can be used (ie - Azure Management Portal), cmdlets for Windows PowerShell, or the Service Management APIs.
- Delete and recreate it whenever needed like any other virtual machine.
- Virtual machines supports the ability to scale up and\or out by configuring autoscaling.

For detailed information on how to manage the virtual machines in Microsoft Azure, see the Virtual Machine Center and also the Downloads at Azure Government site.

Cloud Services

Unlike Virtual Machines, with Cloud Services Microsoft performs the infrastructure services such as Operating system patching, monitoring and scaling so the customer can focus on configuration and maintenance of their applications and data.

When an application is developed and run on Azure, the code and configuration together are called an Azure cloud service. By creating a cloud service, a multi-tier web application can be deployed in Azure, defining multiple roles to distribute processing and allow flexible scaling of applications. A cloud service consists of one or more web roles and/or worker roles, each with its own application files and configuration. Cloud services are used to support more complex multi-tier architectures.

Azure maintains the cloud service infrastructure, performing routine maintenance, patching the operating systems, load balancing and attempting to recover from service and hardware failures. If at least two instances of every role are defined, most maintenance, as well as service upgrades, can be performed without any interruption in service.

Each cloud service has two environments to which service packages and configurations can be deployed. A cloud service can be deployed to the staging environment to test it before you promote it to production. Promoting a staged cloud service to production is a simple matter of swapping the virtual IP addresses (VIPs) that are associated with the two environments.

For detailed information on how to manage the Cloud Services in Microsoft Azure, see the Cloud Services Center and also the Downloads at Azure Government site.

Storage Services

Azure Government Storage Services comprise two classes: *Azure Storage and Azure SQL Databases*. Access to storage accounts and SQL Databases must be explicitly authorized by providing appropriate authorization information to that compute service.

The storage account is a unique namespace that provides access to Azure Storage. Each storage account can contain a combination of blob, queue, and table data. Below is a description of the different storage types:

- **Blob.** A blob can be any type of text or binary data, such as a document, media file, or application installer. Every blob is organized into a container. Containers also provide a useful way to assign security policies to groups of objects. A storage account can contain any number of containers, and a container can contain any number of blobs.
- **Table Storage.** Table storage stores structured datasets and is a NoSQL key-attribute data store, which allows for rapid development and fast access to large quantities of data. Table storage is a key-attribute store, meaning that every value in a table is stored with a typed property name. The property name can be used for filtering and specifying selection criteria.
- **Queue storage.** Queue storage provides a reliable messaging solution for asynchronous communication between application components, whether they are running in the cloud, on

the desktop, on an on-premises server, or on a mobile device. Queue storage also supports managing asynchronous tasks and building process workflows.

The Azure Storage services are designed to be highly available, resilient and scale to customer demands. Therefore, Azure Government provides:

- **Fault- Tolerance -** Windows Azure Blobs, Tables and Queues stored on Windows Azure are replicated three times in the same data center for resiliency against hardware failure.
- **Geo Redundant -** Windows Azure Blobs and Tables are also geo-replicated between two U.S. data centers at least 500 miles apart from each other. This provides additional data durability in the case of a major disaster, or to leverage for read-only operations like reporting and Business Intelligence. For non-critical data, a choice of switching off Geo-replication is provided. Replication occurs over Microsoft's dedicated government network spine and is encrypted in transit.
- **Locally Redundant Storage -** Customers can store non critical data at a reduced cost and lower levels of durability by turning off the default settings for Geo Redundancy in the storage accounts. When Geo Redundancy is turned off, Azure storage still provides fault tolerance and durability at the same levels as three replicas, providing resiliency against hardware failure.
- **Scalable -** Azure Storage is a scalable storage service in the cloud which can auto scale up or down to meet massive volumes.
- **Service Level Agreements -** Azure Storage is a managed service that has a 99.9% monthly uptime SLA.
- **Security -** Azure Storage provides simple security for calls to storage service via HTTPS endpoint and digitally sign requests for privileged operations. More granular security is provided via Shared Access Signatures.
- **Cost Savings –** Azure Storage leverages snapshotting and differencing disk technology to make sure that minimal duplication of data across the storage tiers is leveraged to save costs, but redundancy and protection of the snapshot is maintained.

For additional Storage information refer to the Azure Storage Documentation center, Introduction to Microsoft Azure Storage documentation.

Data Management

The Microsoft Data Management Platform is built on SQL Server technology. SQL Server is the leading provider of database management systems and can be leveraged extensively in Azure Government for multiple applications. The SQL platform extends from customers physical on-

premises machines, private cloud environments, third party hosted private cloud environments, and Azure. This cross environment capability enables customers to better meet unique and diverse business needs through a combination of on-premises and cloud-hosted deployments, while using the same set of familiar server products and development tools across these environments.

Azure Government provides two options for hosting SQL Server-based data in Cloud:

- **SQL Database (Azure SQL Database)** is a relational database-as-a-service and is built on standardized hardware and software that is owned, hosted, and maintained by Microsoft. With SQL Database, customers can develop directly on the service using built-in features and functionality. SQL Database is delivered in Service Tiers to meet cost, performance and disaster recovery requirements. SQL Database service provides a service tier to fully manage geo-synchronized databases across the Azure Government regions, significantly reducing costs and management overhead while increasing enterprise scale and resiliency.
- **SQL Server in Virtual Machine (VM)** allows customers to run SQL Server inside a virtual machine in the Azure Government cloud. This provides all the flexibility of managing and running SQL Server similar to running on premises. When using SQL Server in a VM, customers can either bring their own SQL Server license to Azure or use one of the preconfigured SQL Server images in the Azure portal.

It is also important to note that other data management solutions such as Oracle, MySQL, MongoDB and others could also be leveraged within a Virtual Machine. For additional Data Management information refer to the Azure Data Management site and Understanding Azure SQL on the Azure Documentation center.

Network

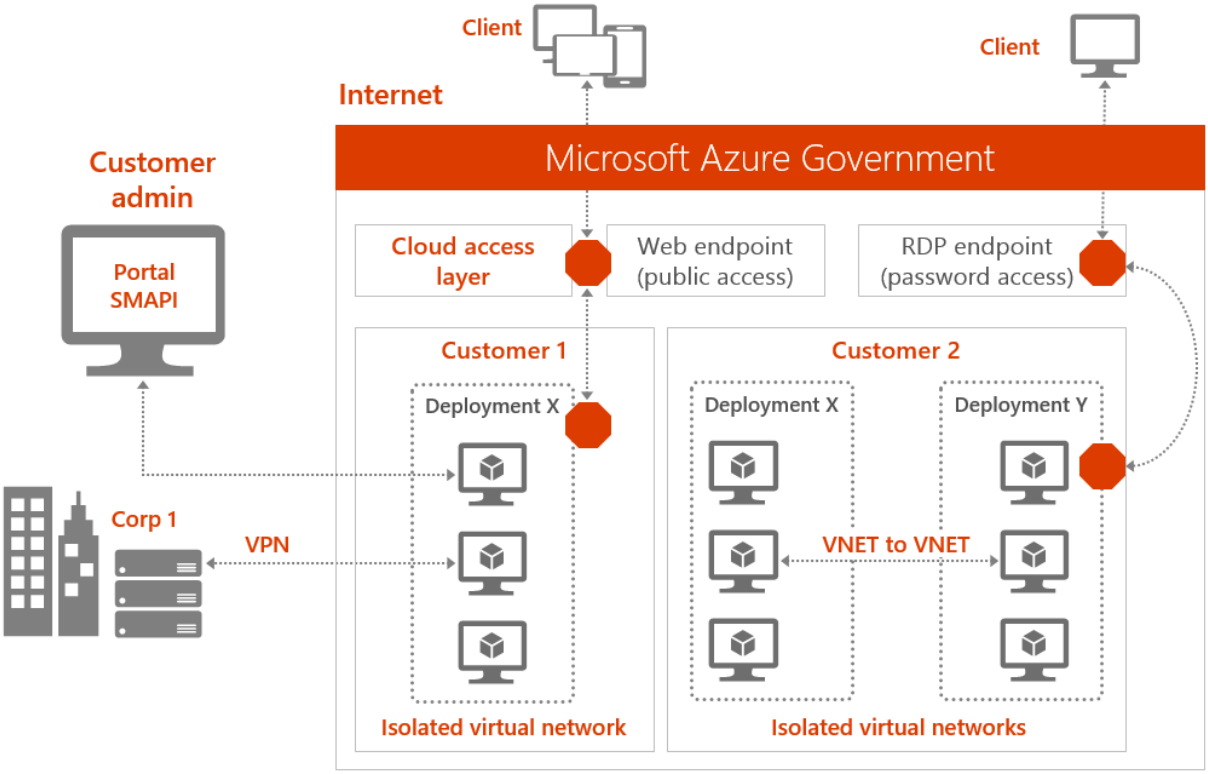
Azure Government maintains a physically isolated network from other Microsoft commercial offerings. Virtual networking provides the capabilities necessary to securely connect VMs to one another and to connect on-premises government data centers with Azure Government VMs. Azure blocks unauthorized traffic to and within Microsoft data centers using a variety of technologies such as firewalls, partitioned Local Area Networks, and physical separation of back-end servers from public-facing interfaces.

Government customers can configure their environments to meet their needs based on:

- **Virtual network**. A customer can assign multiple deployments within a subscription to a virtual network and allow those deployments to communicate with each other using private IP addresses. Each virtual network is isolated from other virtual networks.

- **Network isolation.** Network isolation prevents unwanted tenant-to-tenant communications, and access controls block unauthorized users from the network. Virtual machines do not receive inbound traffic from the Internet unless customers configure them to do so.
- **Encrypting communications.** Built-in cryptographic technology enables customers to encrypt communications within and between deployments and from Azure to on premises data centers. Encryption can be configured to protect administrator access to virtual machines through remote desktop sessions and remote Windows PowerShell. Access to the Azure Management Portal is encrypted by default using HTTPS.

The following diagram illustrates how customers can engage with the Azure Government Network and resources. Network access is provided for developers, administrators and clients.



As the figure shows, Azure Virtual Network lets you create a logical boundary around a group of VMs, called a *virtual network or VNET*, in an Azure Government datacenter. It then allows an IPsec VPN connection to be established between this VNET and the local network. The VMs in a VNET can be created using Azure Virtual Machines, Azure Cloud Services, or both. In other words, they can be VMs created using either the Azure Infrastructure-as-a-Service (IaaS) technology or its Platform-as-a-Service (PaaS) technology.

For additional Storage information refer to the Understanding Virtual Networks on the Azure Documentation center.

Media Services

Azure Media Services allows customers to deliver any media, on virtually any device, anywhere, with the power of Azure. Here are some of the features you can leverage today with Media Services:

On demand encoding: Azure Media Encoder supports a wide variety of studio-grade input and output file formats and is charged based on output gigabytes.

Content Indexing: Allows media files to be accessible and discoverable with speech recognition, transcription, and indexing services.

Content Protection: Industry leading content protection with PlayReady DRM and AES Encryption.

Live Streaming and On demand playback: Microsoft Azure Media Services includes all the tools and services needed to handle media processing, delivery, and consumption

Premium Encoding: Provides decision making logic, new formats and codecs, support for Closed Captioning and many other great features. You can learn more about Premium Encoding here.

For more information on Azure Media Services visit www.azure.com/media

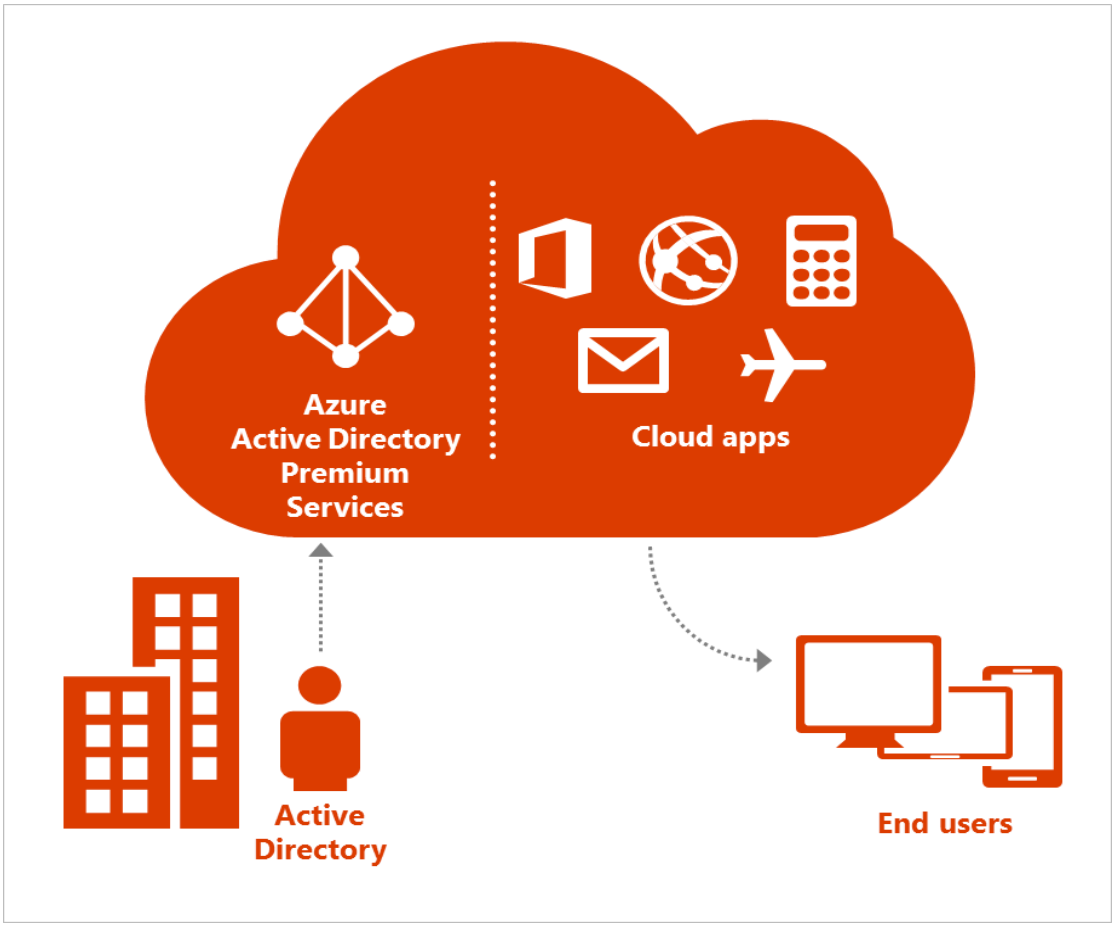
Identity Management

Azure Active Directory (AAD) is a service that provides identity and access management capabilities in Azure Government. In much the same way that Active Directory is a service made available to customers through the Windows Server operating system for on-premises identity management, AAD is a service that is made available through Azure for cloud-based identity management. It also supports Multi-Factor Authentication for additional security. Azure Active Directory maintains a separate Active Directory partition within Azure Government.

AAD enables customers to control access to their environments, data and applications and helps simplify the management of multiple environments and control user access across applications using Single Sign-on. Because it is the customer organization's cloud directory, the customer

can decide who their users are, what information to keep in the cloud, who can use the information or manage it, and what applications or services are allowed to access that information.

Below is a simple representation of ADD integrated with an organizations on-premise Active Directory.



Key ADD capabilities include:

- **Integration with on-premise Active Directory -** Azure AD can be used as a standalone cloud directory for an organization, or existing on premise Active Directory can be integrated with Azure AD. As depicted in the diagram above, Azure AD and on premise AD can be synchronized to provide single sign-on for users and cloud applications such as Office 365 and O365 GCC. Some of the features of integration include directory sync and single sign-on, which further extend the reach of existing on-premises identities into the cloud for an improved admin and end user experience.

- **Integration with customer's applications** - Application developers can integrate their applications with Azure AD to provide single sign-on functionality for their users. This enables enterprise applications to be hosted in the cloud and to easily authenticate users with corporate credentials. It also enables software-as-a-service (SaaS) providers to make authentication easier for users in Azure AD organizations when authenticating to their services. Azure AD supports SAML 2.0, OAuth 2.0, OpenID, and WS-Federations.
- **Strong authentication**. Azure Multi-Factor Authentication is designed to provide an extra layer of authentication, in addition to a user's account credentials, to secure employee, customer, and partner access. Azure Multi-Factor Authentication can be used for both on-premises and cloud applications.

Microsoft's Azure Active Directory runs in the cloud with high scale, high availability, and integrated disaster recovery, while fully respecting the customers' requirements for the privacy and security of their organization's information.

For additional Identity Management information refer to the Active Directory and Multi-Factor Authentication documentation.

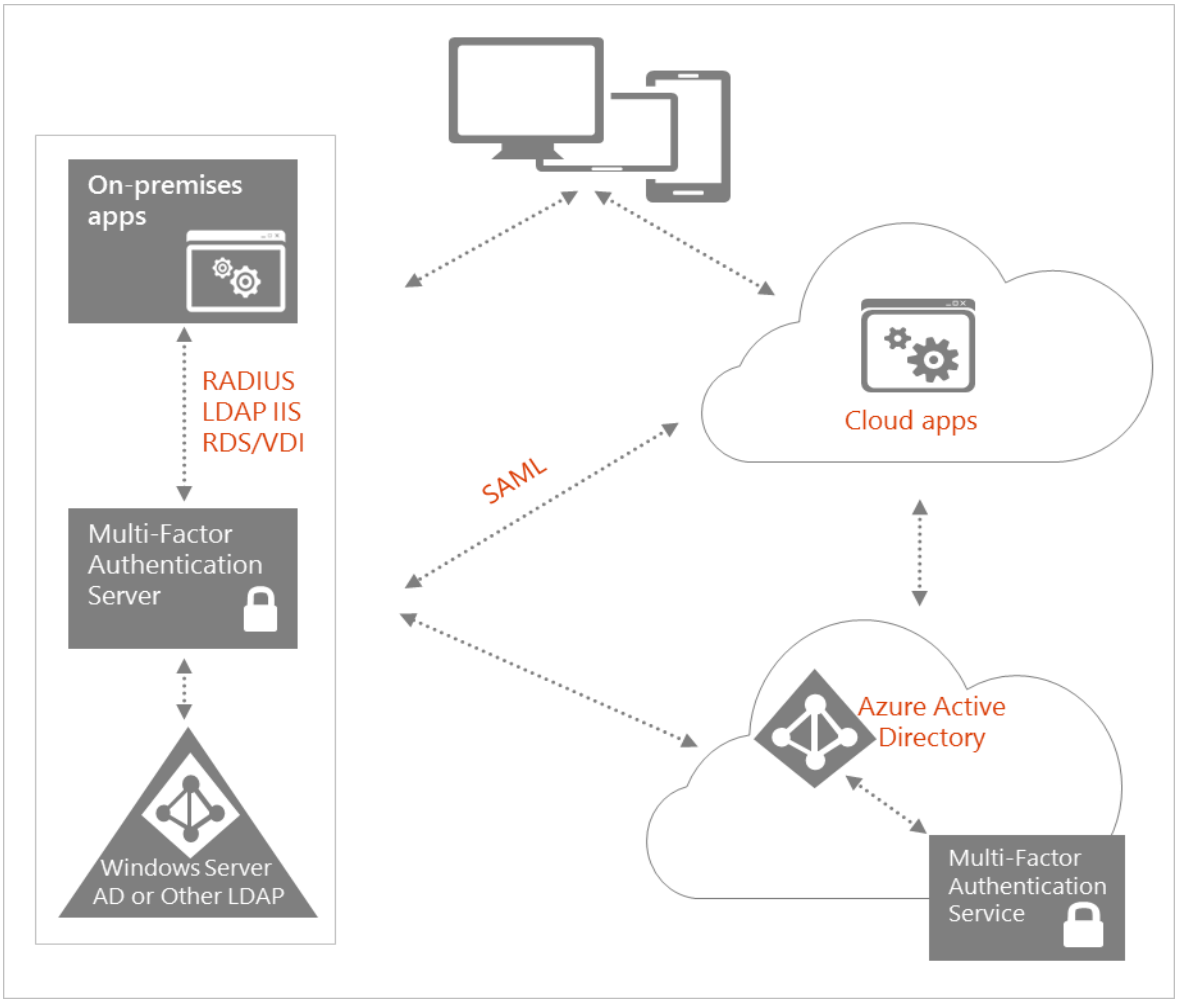
Azure Government Services Implementation Scenarios

This section provides sample scenarios using Azure Government core services. This is only a primer to begin to describe the extensive capabilities and implementations that can help meet a government organization's needs.

Scenario 1: Providing identity federation

Customers can use the Azure Active Directory (AAD) capabilities to establish a single sign-on approach across their on premise and cloud services by integrating Azure Active Directory, on premise Active Directory and Multi-Factor Authentication. It also provides the ability to leverage open authentication standards like oAuth and SAML to federate and provide single sign on across many other cloud based applications and web frameworks.

Below is an overview of a single sign-on implementation with multi-factor support via phone, text and other mechanisms.



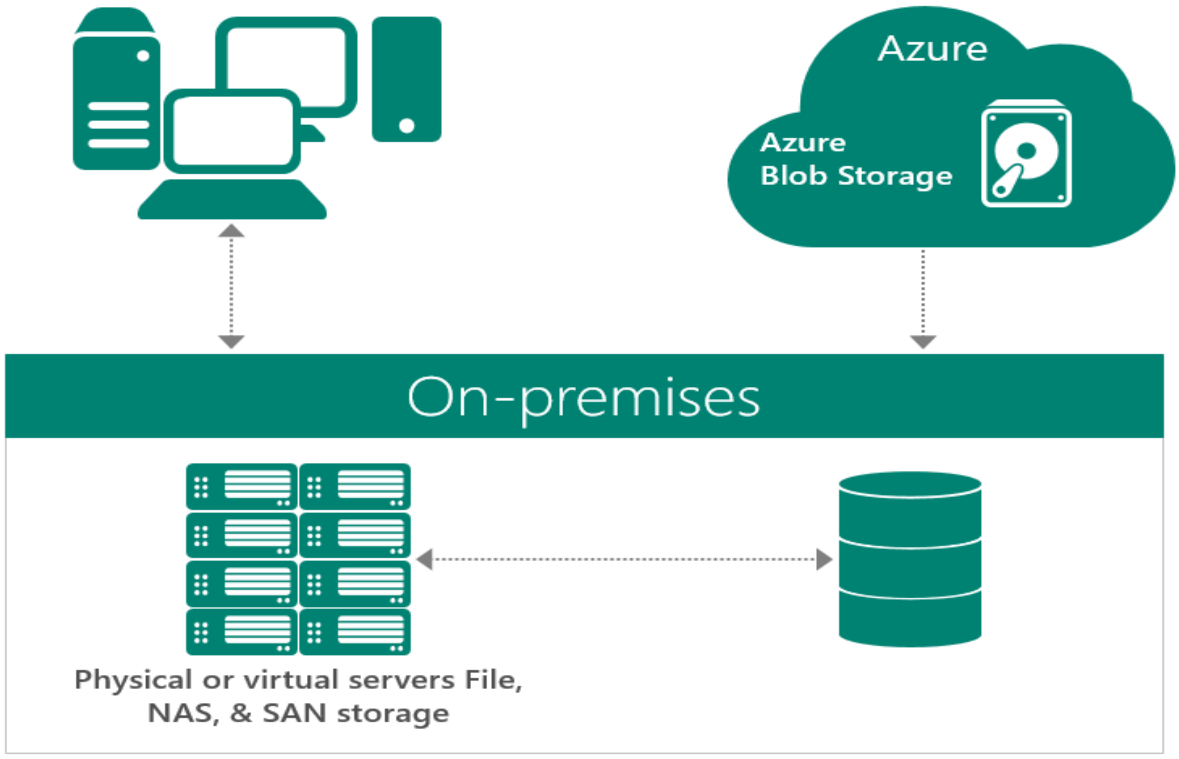
For additional information, refer to Azure Active Directory and Multi-Factor Authentication scenarios on the Azure Trust Center.

Scenario 2: Data Storage, Backup & Recovery

Customers can leverage the Azure Government environment and storage capabilities to securely back up on premise and cloud data and provide a reliable, inexpensive and scalable solution with zero capital investment and minimal operational expense. Other benefits include fault tolerance, geo-redundancy and a 99.9% system uptime service level agreements.

Azure Government provides redundancy within the local datacenter via Locally Redundant Storage (LRS) which means the data is replicated 3 times across the datacenter. Customers may also optionally choose to select Geo-Redundant Storage (GRS) and Read-Access Geo-Redundant Storage (RA-GRS) which will replicate the data across datacenters. This low cost, easy to configure option provides enormous savings and benefits when looking at reporting and disaster recovery requirements.

The below diagram highlights the basic design to store and retrieve large amounts of unstructured data with blobs, tables, queues, files, and SQL Server continuity between on premise and Azure.



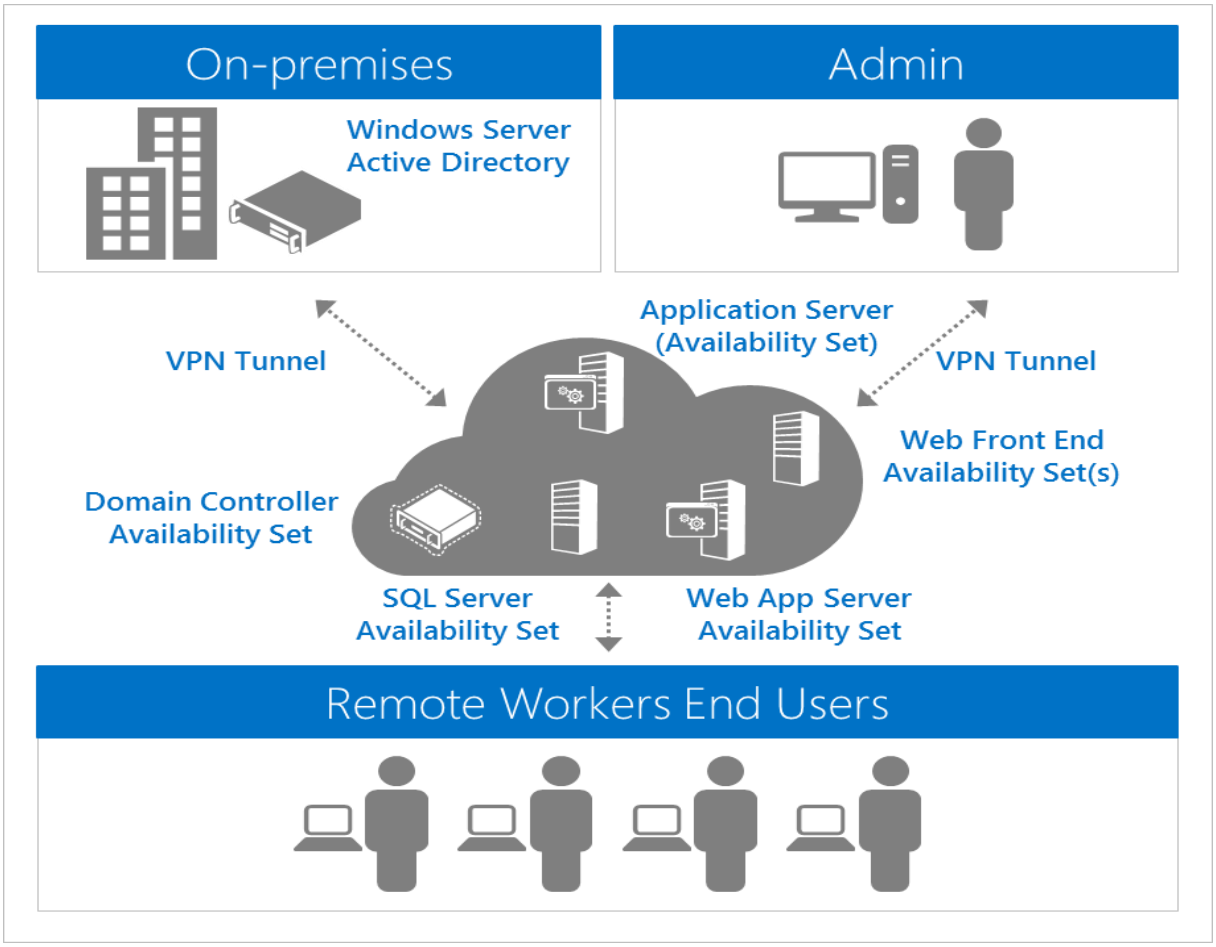
For additional information, refer to Azure Storage.

Scenario 3: Deploying Packaged Applications such as SQL & SharePoint

Many customers desire to run SQL and SharePoint workloads in the Azure Government Cloud. Implementations can be quickly set up and deployed either to provision new infrastructure or to expand an existing one. Azure SQL can also be used for redundancy using SQL Server Always-On which is supported across hybrid datacenters. SQL Server can also perform direct backup to Azure Government. For organizations that need to scale up and down as business workflow demands change, organizations can scale SQL and SharePoint resources on demand, paying only for what they use.

The below example demonstrates configurations for SharePoint and SQL Server running in Azure Government. Also, these environments can be accessed via cloud or on-premise VPN connectivity.

Host SharePoint Server in Azure Government:

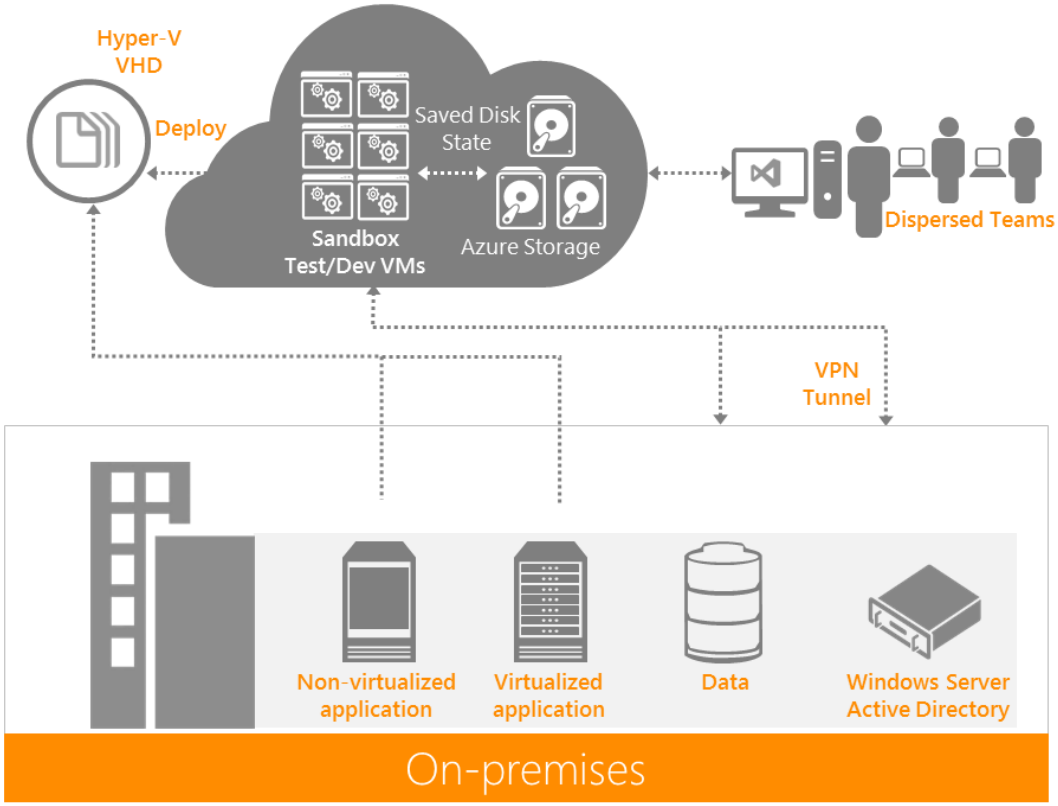


For additional information on SharePoint- based scenarios, please refer to the SharePoint Deployment on Azure Virtual Machines white paper. For SQL scenarios refer to Azure Data Management.

Scenario 4: Quickly Deploy Development and Test Applications

Every software developer needs the infrastructure to design, develop, test, and deliver custom applications. Microsoft Azure provides everything a customer needs to build complete, on-demand environments for application development on Windows, Linux, and any other technology stack—in minutes.

Below is an overview of a provisioned development and testing environment for developing cloud applications on Azure Government. In addition, there is an example of how to provision virtual machines using the Quick Create feature and an image selected and configured from the gallery.



Below is an example of how to quickly create a quick, pre-configured instance, of Windows Server 2012 and an example of how to select and configure a new Windows Server 2012 R2 Datacenter image from the Azure Gallery.

Quick Create:

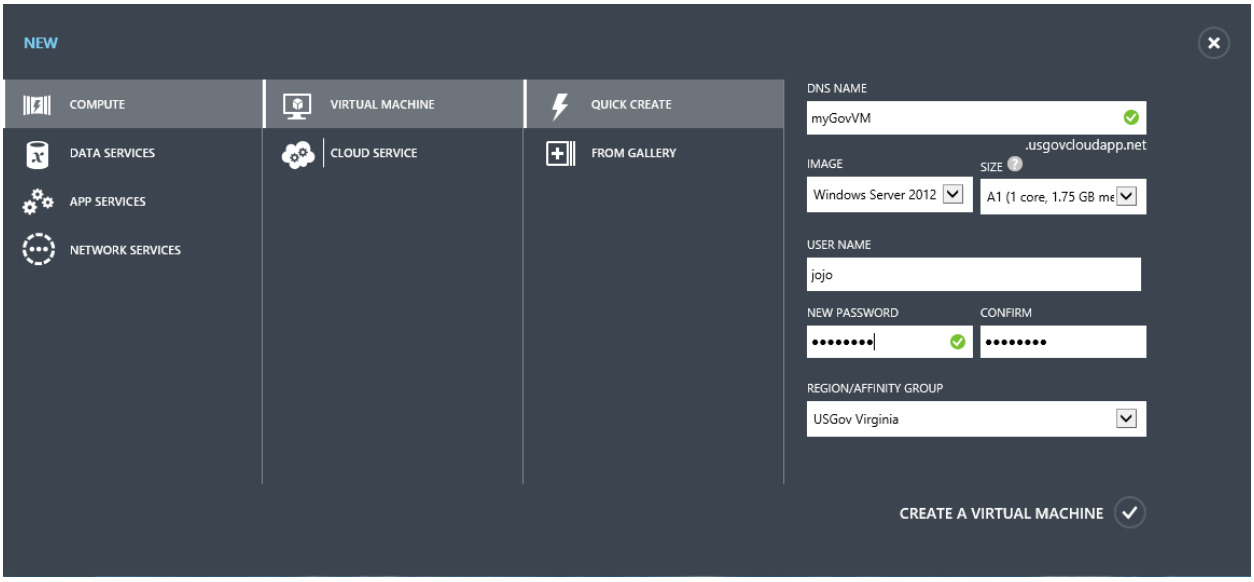
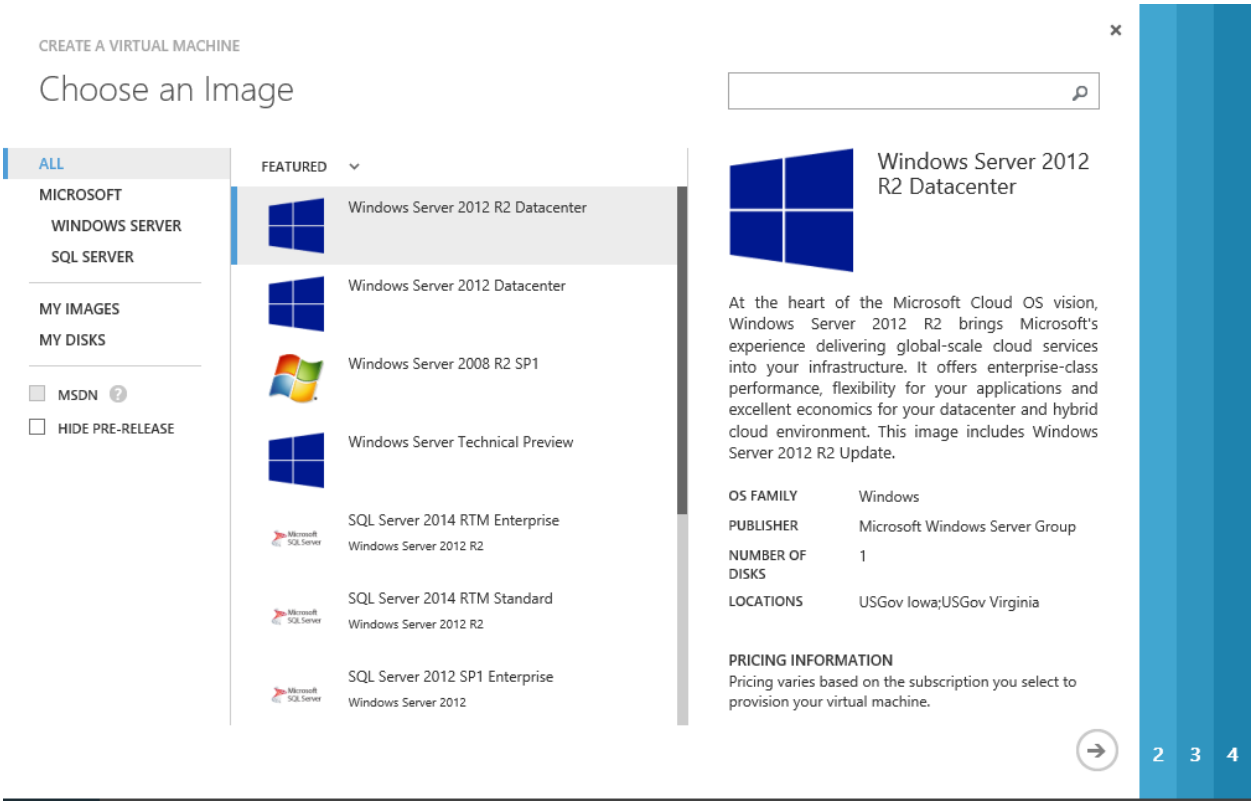


Image Selected and Configured from Gallery:



For additional information, refer to the Azure Documentation center on [how to create Cloud development and test environments](#).

Azure Government Security, Privacy and Compliance Overview

Azure Government works closely with government customers and organizations to develop cutting-edge security, privacy and compliance practices that run some of the largest online services around the globe. Microsoft has made significant investments in building and maintaining a team of security, privacy, and compliance subject matter experts. These teams focus on ensuring Microsoft Azure Government meets its own security and compliance obligations as well as helping customers meet their own compliance requirements. In addition, the compliance team represents the "customer voice" and drives necessary changes in engineering, operations, and relationships with regulatory bodies to help ensure customers' security needs are met.

Security

Azure Government delivers a trusted foundation on which customers can design, build and manage their own secure cloud applications and infrastructure. It also provides transparent accountability to allow customers and their agents to track administration of applications and infrastructure, by themselves and by Microsoft. Below are the key security control areas that Microsoft has invested in.

Infrastructure Protection

Azure infrastructure includes hardware, software, administrative and operations staff, and physical data centers. Azure addresses security risks 24X7 across its infrastructure with continuous intrusion detection and prevention systems, denial of service attack prevention, regular penetration testing, and forensic tools that help identify and mitigate threats. With Azure, customers can reduce the need to invest in these capabilities on their own and benefit from economies of scale in Microsoft datacenter infrastructure.

- **24 hour monitored physical security -** Datacenters are physically constructed, managed, and monitored to shelter data and services from unauthorized access as well as environmental threats.
- **Monitoring and logging -** Security is monitored with the aid of centralized monitoring, correlation, and analysis systems that manage the large amount of information generated by devices within the environment and providing timely alerts.
- **Patching -** Integrated deployment systems manage the distribution and installation of security patches. Customers can apply similar patch management processes for Virtual Machines deployed in Azure.
- **Antivirus/Antimalware protection -** Microsoft Antimalware is built-in to Cloud Services and can be enabled for Virtual Machines to help identify and remove viruses, spyware and other malicious software and provide real time protection. Customers can also run antimalware solutions from partners on their Virtual Machines.
- **Intrusion detection and DDoS -** Intrusion detection and prevention systems, denial of service attack prevention, regular penetration testing, and forensic tools help identify and mitigate threats from both outside and inside of Azure.
- **Penetration testing -** Microsoft conducts regular penetration testing to improve Azure security controls and processes. Microsoft understands that security assessment is also an important part of a customers' application development and deployment. Therefore, Microsoft has established a policy for customers to carry out authorized penetration testing on their applications hosted in Azure

Network Protection

Azure networking provides the infrastructure necessary to securely connect VMs to one another and to connect on-premises data centers with Azure VMs. Azure blocks unauthorized traffic to and within Microsoft data centers using a variety of technologies such as firewalls, partitioned Local Area Networks, and physical separation of back-end servers from public-facing interfaces.

- **Network isolation.** Network isolation prevents unwanted tenant-to-tenant communications, and access controls block unauthorized users from the network. Virtual machines do not receive inbound traffic from the Internet unless customers configure them to do so.
- **Virtual networking.** A customer can assign multiple deployments within a subscription to a virtual network and allow those deployments to communicate with each other using private IP addresses. Each virtual network is isolated from other virtual networks.

- **Encrypting communications.** Built-in cryptographic technology enables customers to encrypt communications within and between deployments, between Azure regions, and from Azure to on premise data centers. Encryption can be configured to protect administrator access to virtual machines through remote desktop sessions and remote Windows PowerShell. Access to the Azure Management Portal is encrypted by default using HTTPS.

Identity and Access

Azure Active Directory is a comprehensive identity and access management solution in the cloud. It combines core directory services, advanced identity governance, security, and application access management. Azure Active Directory makes it easy for developers to build policy-based identity management into their applications.

- **Access monitoring and logging -** Security reports are used to monitor access patterns and to proactively identify and mitigate potential threats. Microsoft administrative operations, including system access, are logged to provide an audit trail if unauthorized or accidental changes are made. Customers can turn on additional access monitoring functionality in Azure and use third-party monitoring tools to detect additional threats. Customers can request reports from Microsoft that provide information about user access to their environments.
- **Strong authentication -** Azure Multi-Factor Authentication reduces organizational risk and helps enable regulatory compliance by providing an extra layer of authentication, in addition to a user's account credentials, to secure employee, customer, and partner access. Azure Multi-Factor Authentication can be used for both on-premises and cloud applications.
- **Role-based access control -** Multiple tools in Azure support authorization based on their role, simplifying access control across defined groups of users.

Data Protection

Both technological safeguards, such as encrypted communications, and operation processes help keep Customer Data secure. Customers have the flexibility to implement additional encryption and manage their own keys.

- **Data in transit.** Azure uses industry-standard transport protocols such as SSL and TLS between user devices and Microsoft data centers, and within data centers themselves. With virtual networks, customers can use industry standard IPsec protocol to encrypt traffic between their corporate VPN gateway and Azure. Customers can enable encryption for traffic between their own VMs and end users.

- **Data at rest.** Customers are responsible for ensuring that data stored in Azure is encrypted in accordance with their standards. Azure offers a wide range of encryption capabilities up to AES-256, giving customers the flexibility to choose the solution that best meets their needs. Options include .NET cryptographic services, Windows Server public key infrastructure (PKI) components, Active Directory Rights Management Services (AD RMS), and BitLocker for data import/export scenarios.
- **Data segregation.** Azure is a multi-tenant service, meaning that multiple customers' deployments and virtual machines are stored on the same physical hardware. Azure uses logical isolation to segregate each customer's data from that of others. This provides the scale and economic benefits of multitenant services while rigorously preventing customers from accessing one another's data.
- **Data destruction.** When customers delete data or leave Azure, Microsoft follows strict standards for overwriting storage resources before reuse, as well physical destruction of decommissioned hardware.

For additional security information refer to the security best practices or Azure Security Insights documents on Azure Trust Center.

Privacy

Microsoft has implemented strong privacy protections in Azure Government services and is committed to safeguarding the privacy of customer data. In addition, Microsoft strives to be transparent in service management so customers have visibility into where their data resides and who has access to it. Microsoft has adopted several approaches to achieve the highest levels of Privacy including:

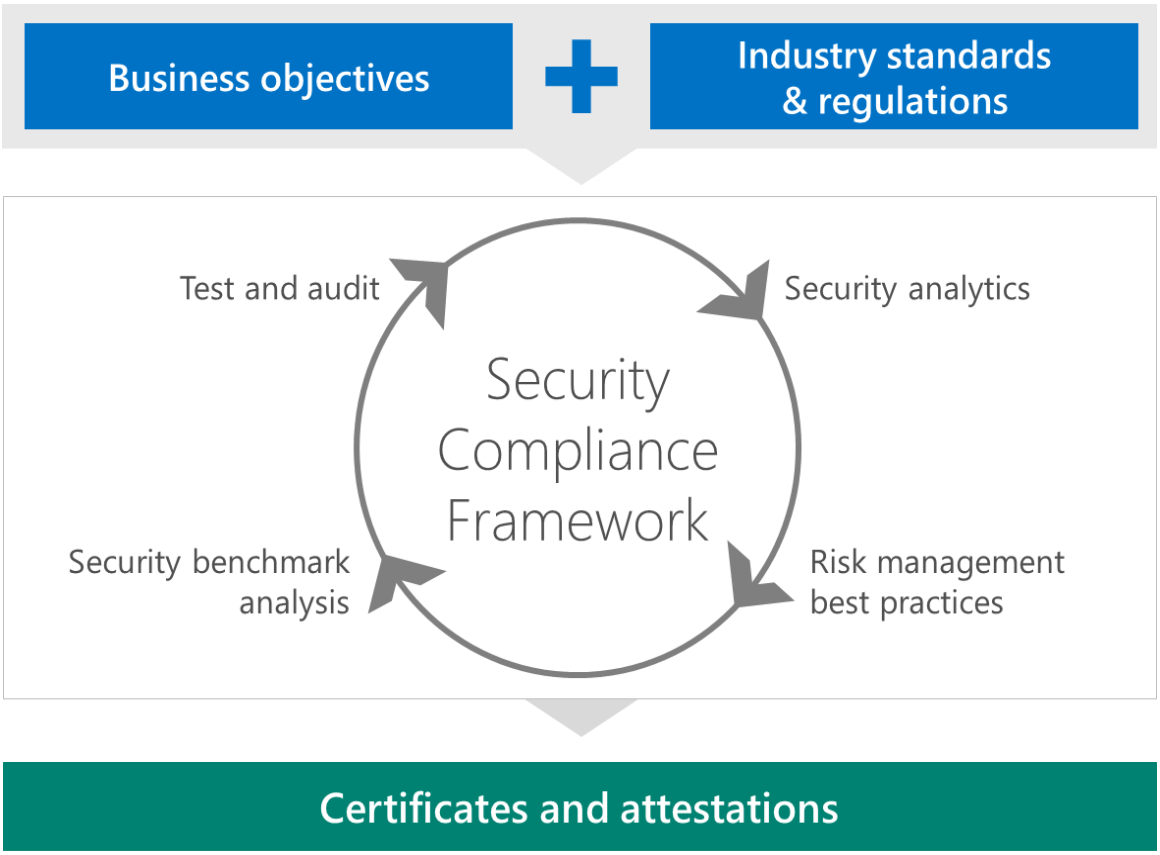
- **Privacy by Design -** With Microsoft, customers can expect Privacy by Design, which describes not only how Microsoft builds products and services, how services are operated, and how internal teams are organized to support privacy.
- **Restricted data access and use -** Access to customer data by Microsoft personnel is restricted. Customer data is only accessed when necessary to support the customer's use of Azure. This may include troubleshooting aimed at preventing, detecting or repairing problems affecting the operation of Azure and the improvement of features that involve the detection of, and protection against, emerging and evolving threats to the user (such as malware or spam). When granted, access is controlled and logged. Strong authentication, including the use of multi-factor authentication, helps limit access to authorized personnel only. Access is revoked as soon as it is no longer needed.

- **Contractual commitments -** Microsoft has cloud service-specific privacy statements and makes contractual commitments to safeguard customer data and provide privacy protections.
- **Control over data location -** For many customers, knowing and controlling the location of their data can be an important element of data privacy compliance and governance. Azure customers can specify the U.S. geographic areas where their customer data is stored. Data may be replicated within a geographic area for redundancy, but will not be transmitted outside it.
- **No use for advertising -** Azure does not share Customer Data with its advertiser-supported services. Microsoft also does not mine customer data for advertising.

Compliance

Microsoft has been actively engaged in designing and testing of cloud compliance requirements for Public Sector standards and requirements and establishing itself as an integral part of the government assurance and security ecosystem. This includes a commitment to industry leading certifications such as the *United States Federal Risk and Authorization Management Program (FedRAMP), Defense Information Systems Agency (DISA)/Enterprise Cloud Service Broker (ECSB), Criminal Justice Information Services Division (CJIS), and Health Insurance Portability and Accountability Act (HIPAA).*

Microsoft's compliance framework contains test and audit phases, security analytics, risk management best practices, and security benchmark analysis to achieve certifications and attestations as described below. It uses a continuous compliance processes to make it easier for Microsoft to achieve and maintain its certifications and it enables customers to get the same high level of compliance readiness across multiple services to meet their changing needs efficiently. Together, security-enhanced technology and effective compliance processes enable Microsoft and government customers to maintain and expand certifications.



Microsoft is committed to ongoing verification by third party audit firms, and shares audit report findings and compliance packages with government customers to help them fulfill their own compliance obligations. For example:

- Microsoft publishes best practices and prescriptive guidance on securing customer data, applications, and infrastructure in Microsoft Azure.
- Microsoft provides detailed information about Microsoft Azure security, privacy, and compliance in available online at the Azure Trust Center. This includes a list of current certifications, links to whitepapers, and other detailed information.
- Microsoft participates in industry-wide transparency initiatives and government assurance initiatives organizations such as the Cloud Security Alliance (CSA).
- Microsoft publishes reports a Security Response Center Progress report and a Security Intelligence report to provide insight to customers into the threat landscape.

By providing customers with compliant cloud services and detailed information about how it addresses security standards across a range of compliance programs, Microsoft make it easier

for customers to achieve compliance for the infrastructure and applications they run in Microsoft Azure Government.

Download the Azure Security, Privacy, and Compliance whitepaper to learn more.

Summary

Azure Government is the next step in Microsoft's One Government cloud evolution to help U.S. government organizations to find more effective ways to engage with their citizens and to achieve better cross-agency collaboration. This will allow agencies to accelerate their IT organizations agility, minimize datacenter investments, and still maximize existing investments by adopting a hybrid cloud approach. All, while still meeting higher levels of security, privacy and compliance requirements.

Microsoft and Azure Government Cloud provides a deep, tenured commitment to innovation, industry leadership, security, privacy, and compliance, and delivers a trusted Government Community Cloud that enables government organizations and their partners to realize the benefits of cloud speed, scale, and economics. Azure Government also provides an interoperable cloud platform, with products and technologies that are open from the ground up - creating a platform that provides choice to meet business and technology needs.

To learn more about Azure Government Cloud, visit the Microsoft Azure Government website and the Azure Government Developer Guide.

Appendix A: References and Further Reading

The following resources are available to provide more general information about Microsoft Azure Government and related Microsoft services, as well as specific items referenced in the main text:

Azure FedRAMP P-ATO Documentation

(Available through the FedRAMP Package request form)

Azure Government Home – general information about Azure Government

http://azure.microsoft.com/en-us/features/gov/

Microsoft Azure Government Documentation

http://azure.microsoft.com/en-us/documentation/

Microsoft Azure Government Downloads

http://azure.microsoft.com/en-us/downloads/

Microsoft Azure Trust Center Resources – Azure Downloadable whitepapers

http://azure.microsoft.com/en-us/support/trust-center/resources/

Microsoft's Security Development Lifecycle (SDL)

http://www.microsoft.com/security/sdl/

Azure Government Developer Guide

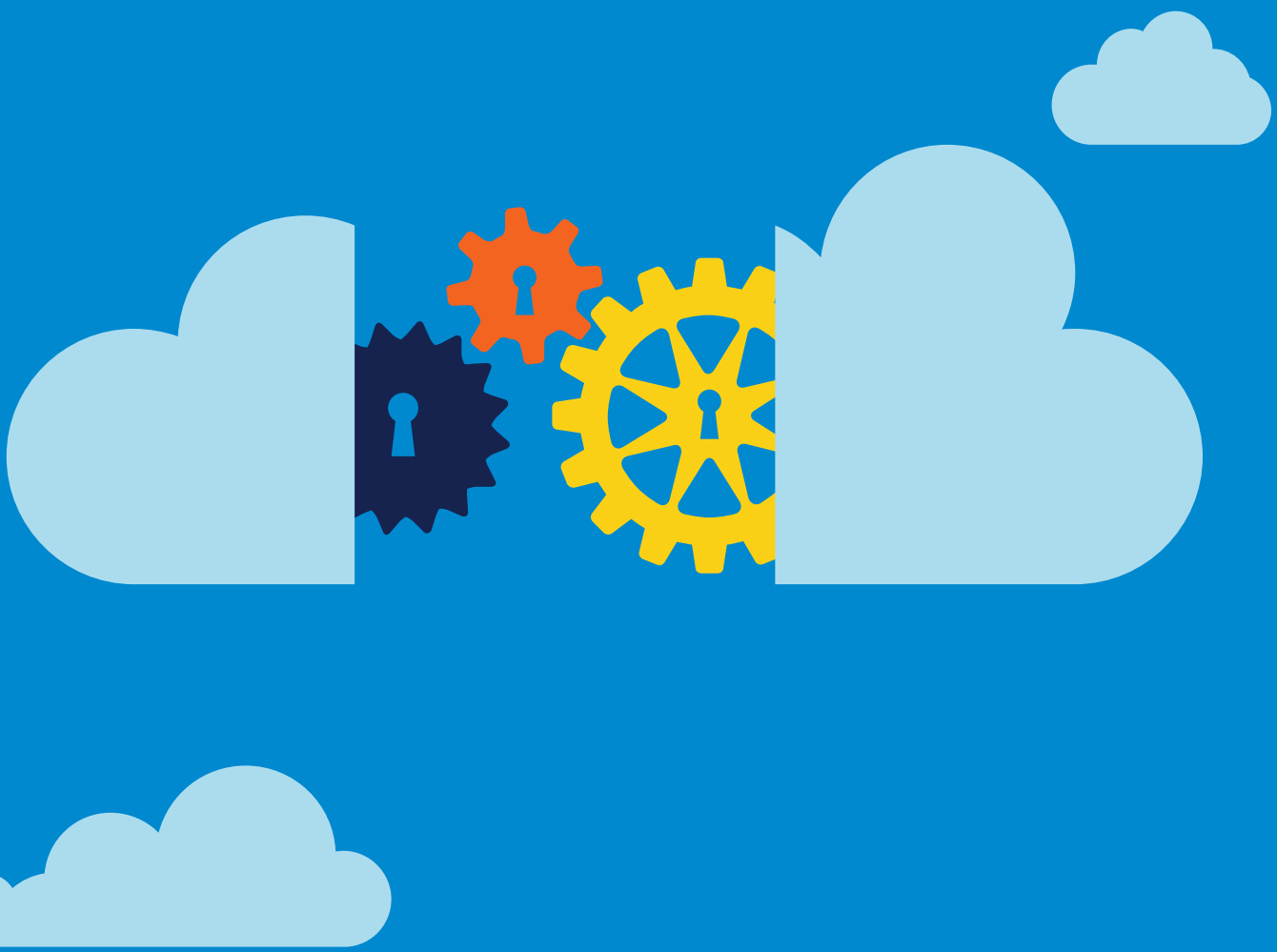
http://azure.microsoft.com/en-us/documentation/articles/azure-government-developer-guide/

Nasuni - 2013 State of the Cloud Storage

http://www.nasuni.com/resource/the-state-of-cloud-storage-in-2013

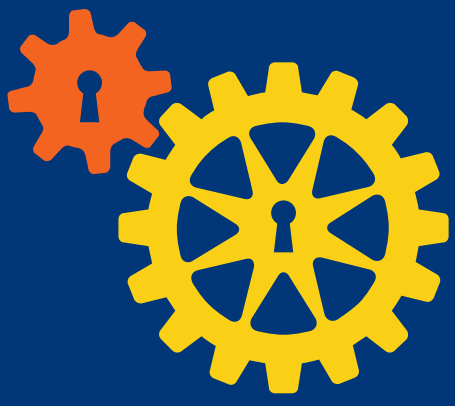
Trusted Cloud: Microsoft Azure Security, Privacy, and Compliance

April 2015



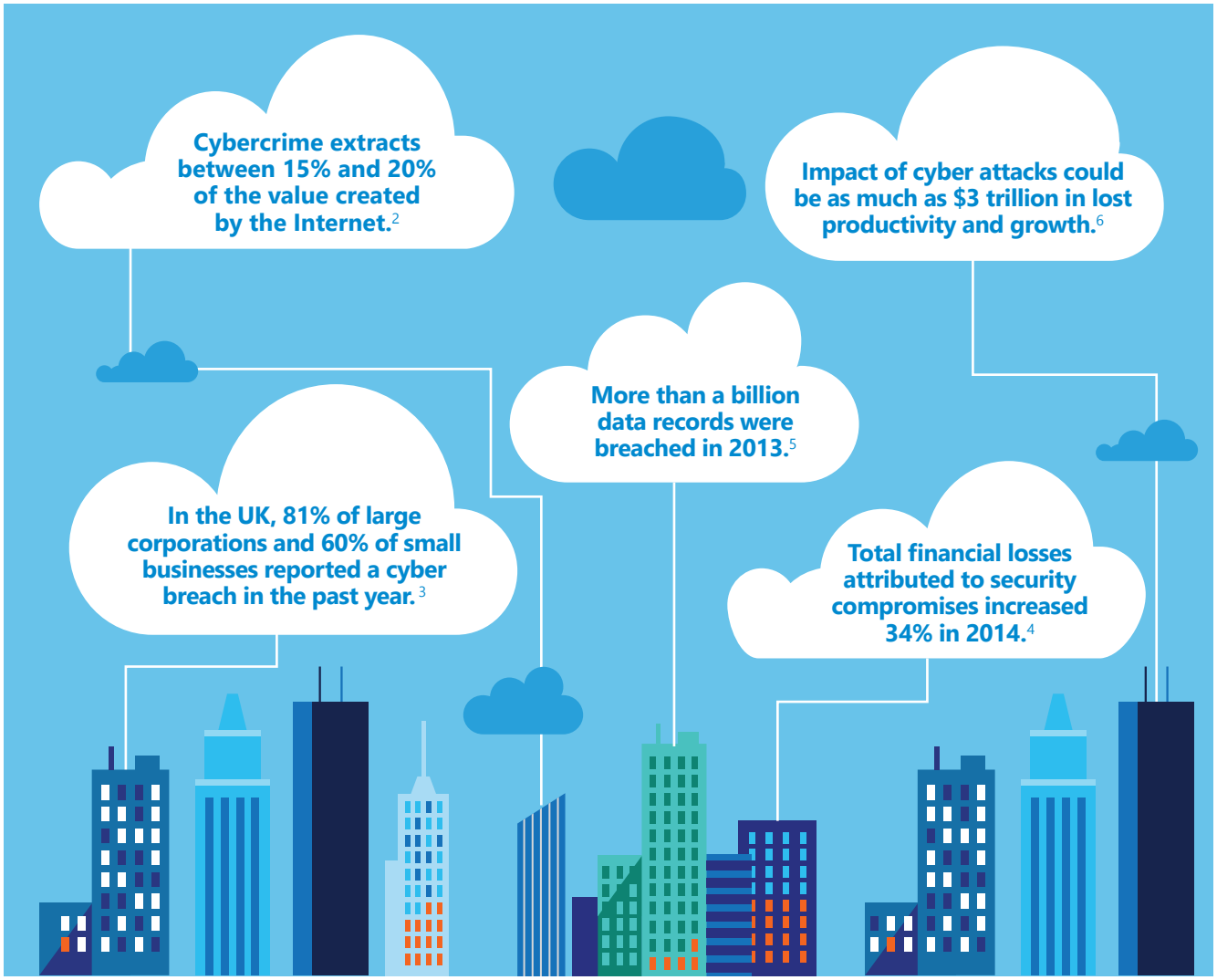
Microsoft

Contents



Introduction

With the emergence of cloud computing, today's IT organizations are playing an increasingly important role in driving business strategy. While cost reduction is still a top priority, scalability and business agility have stepped to the forefront for IT decision makers. As a result, spending on cloud solutions is expected to grow 30 percent from 2013 to 2018, compared with 5 percent overall growth for enterprise IT. And cloud services are keeping pace[1]. Analysts expect to see a ten-fold increase in the number of cloud-based solutions on the market in the next four to five years.



Sources:

1 Forbes, "Roundup of Cloud Computing Forecasts and Market Estimates, 2015," 1/24/2015. http://aka.ms/forbes-cloud-2015

2 Intel/McAfee, "Net Losses: Estimating the Global Cost of Cybercrime," June 2014. http://aka.ms/mcafee-cybercrime-report

3 UK Dept. for Business, Innovation and Skills, "2014 Information Security Breaches Survey." http://aka.ms/uk-gov_breach-survey

4 PWC, "Global State of Information Security Survey: 2015." http://aka.ms/pwc-cybercrime

5 Gemalto, 2014 Breach Level Index Report

6 McKinsey & Company, report for World Economic Forum, Jan. 2014

Still, many CIOs hesitate to fully embrace a cloud-first approach. Their hesitation stems in part from anxiety over a wide range of privacy and security related issues. Large-scale data breaches dominated headlines in 2014 and continue in the news today, raising a critical question for IT leaders everywhere: How can organizations build scalable cloud solutions and increase business agility while taking the necessary steps to secure our data and ensure privacy and compliance across the enterprise?

Without a clear answer, security concerns threaten to stall innovation and stifle business growth. IT and business leaders need a trusted partner to bridge the gap between innovation and security. With the right technologies and processes, even the most complex enterprise can move to the cloud with confidence.

"71% of strategic buyers cite scalability, cost and business agility as the most important drivers for using cloud services."

Gigaom Research

What customers want from cloud providers

Every business has different needs and every business will reap distinct benefits from cloud solutions. Still, customers of all kinds have the same basic concerns about moving to the cloud. They want to retain control of their data, and they want that data to be kept secure and private, all while maintaining transparency and compliance.

Secure our data. The scale and scope of intrusions are growing. In 2014, cyber criminals compromised more than a billion data records in more than 1500 breaches.[7] In a 2014 report for the World Economic Forum[8] , McKinsey & Company estimated the risk of cyberattacks "could materially slow the pace of technology and business innovation with as much as $3 trillion in aggregate impact." In any security attack, target organizations are only as safe as their weakest link. If any component is not secured, then the entire system is at risk. While acknowledging that the cloud can provide increased data security and administrative control, IT leaders are still concerned that migrating to the cloud will leave them more vulnerable to hackers than their current in-house solutions.

Keep our data private. Cloud services raise unique privacy challenges for businesses. As companies look to the cloud to save on infrastructure costs and improve their flexibility, they also worry about losing control of where their data is stored, who is accessing it, and how it gets used. Since the revelations of widespread surveillance by the US government in 2013, privacy concerns have become more accentuated, and the cloud has come under greater scrutiny as a result.

Give us control. Even as they take advantage of the cloud to deploy more innovative solutions, companies are very concerned about losing control of their data. The recent disclosures of government agencies accessing customer data, through both legal and extralegal means, make some CIOs wary of storing their data in the cloud. Many companies are therefore looking to choose where their data resides in the cloud and to control what entities have visibility into that data.

Promote transparency. While security, privacy, and control are important to business decision makers, they also want the ability to independently verify how their data is being stored, accessed, and secured. Businesses understand that they cannot control what they cannot see. To create this sort of visibility for customers, cloud providers must offer transparency of their security, privacy and compliance practices and actions to give customers the information they need to make their own decisions.

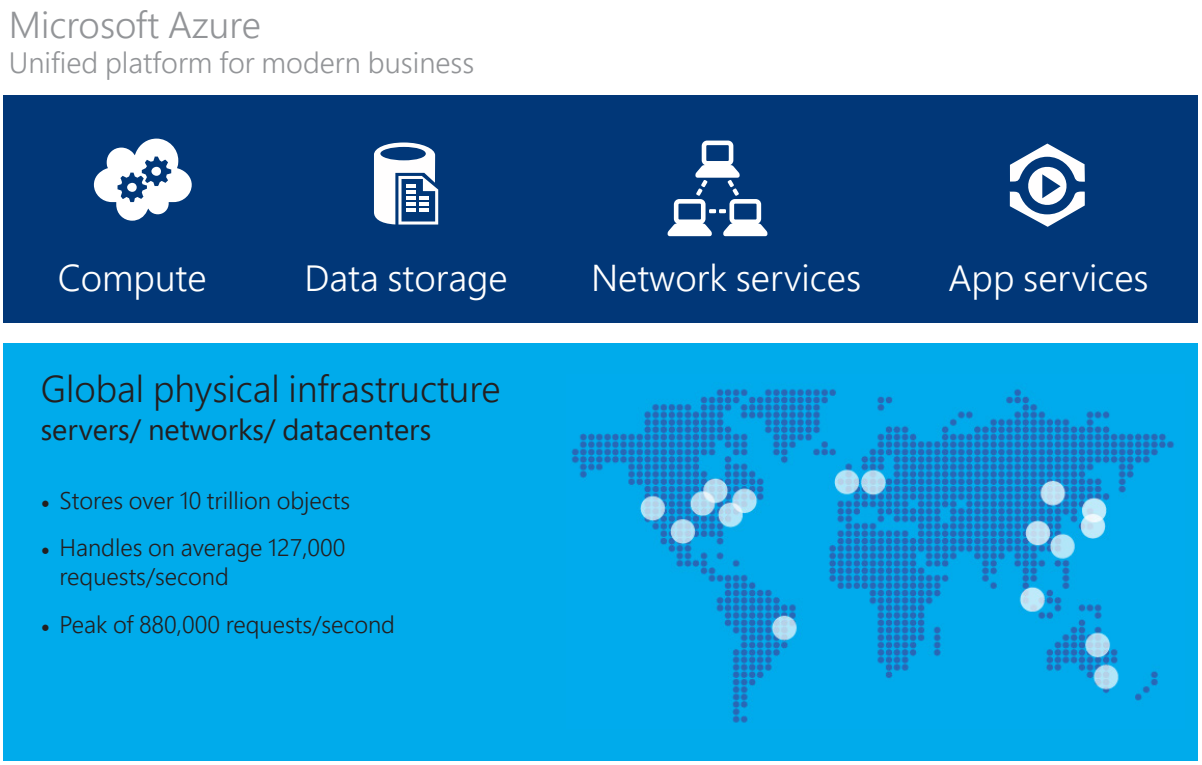
7 Gemalto, 2014 Breach Level Index Report

8 McKinsey & Company, for World Economic Forum, Jan. 2014

Maintain compliance. As companies and government agencies expand their use of cloud technologies, the complexity and scope of standards and regulations continues to evolve. Companies need to know that their compliance standards will be met, and that compliance will evolve as regulations change over time.

Microsoft Azure: Built for trust

Microsoft Azure provides cloud services for a wide range of enterprise and government customers. The core of Microsoft Azure provides four primary functions on which customers build and manage virtual environments, applications, and associated configurations.



Microsoft, with its unique experience and scale, delivers these services to many of the world's leading enterprises and government agencies. Today, the Microsoft cloud infrastructure supports over 1 billion customers across our enterprise and consumer services in 140 countries and supports 10 languages and 24 currencies. Drawing on this history and scale, Microsoft has implemented software development with enhanced security, operational management, and threat mitigation practices, helping it to deliver services that achieve higher levels of security, privacy, and compliance than most customers could achieve on their own.

Microsoft shares best practices with government and commercial organizations and engages in broad security efforts through the creation of centers of excellence, including the Microsoft Digital Crimes Unit, Microsoft Security Response Center, and Microsoft Malware Protection Center.

Security: Working to keep customer data safe

Azure can help reduce the cost, complexity, and risk associated with security and compliance in the cloud. A survey funded by Microsoft and performed by ComScore[9] found that while many organizations have initial concerns about moving to the cloud, a majority of cloud adopters reported that they achieved significant security benefits. These security benefits are reported because few individual organizations can replicate the technology and operational processes that Microsoft uses to help safeguard its enterprise cloud services and comply with a wide range of international standards. When companies use Azure, they benefit from Microsoft's unmatched scale and experience running compliant online services around the globe. Microsoft's expertise becomes the customer's expertise.

Initial concern

60% cited concerns around data security as a barrier to adoption

45% concerned that the cloud would result in a lack of data control

Realized benefit

94% experienced security benefits they didn't previously have on-premise

62% said privacy protection increased as a result of moving to the cloud

Microsoft Cloud Experience:

- 200+ cloud services
- 1+ million servers
- $15B+ infrastructure investment
- 1 billion customers
- 20 million businesses
- 140 countries worldwide

Security Design and Operations

Secure cloud solutions are the result of comprehensive planning, innovative design, and efficient operations. Microsoft makes security a priority at every step, from code development to incident response.

Design for security from the ground up. Azure code development adheres to Microsoft's Security Development Lifecycle (SDL). The SDL is a software development process that helps developers build more secure software and address security compliance requirements while reducing development cost. The SDL became central to Microsoft's development practices a decade ago and is shared freely with the industry and customers. It embeds security requirements into systems and software through the planning, design, development, and deployment phases.

9 http://aka.ms/twc-cloud-trust-study

Enhancing operational security. Azure adheres to a rigorous set of security controls that govern operations and support. Microsoft deploys combinations of preventive, defensive, and reactive controls including the following mechanisms to help protect against unauthorized developer and/or administrative activity:

- Tight access controls on sensitive data, including a requirement for two-factor smartcard-based authentication to perform sensitive operations.
- Combinations of controls that enhance independent detection of malicious activity.
- Multiple levels of monitoring, logging, and reporting.

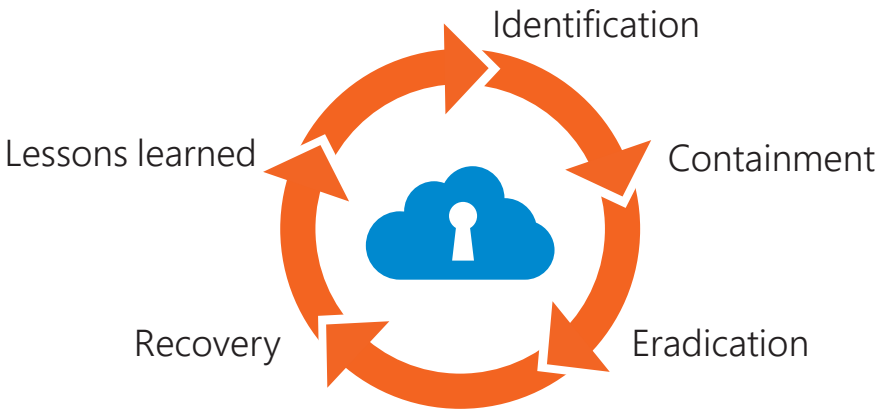
Additionally, Microsoft conducts background verification checks of certain operations personnel and limits access to applications, systems, and network infrastructure in proportion to the level of background verification.

Assume breach. One key operational best practice that Microsoft uses to harden its cloud services is known as the "assume breach" strategy. A dedicated "red team" of software security experts simulates real-world attacks at the network, platform, and application layers, testing Azure's ability to detect, protect against, and recover from breaches. By constantly challenging the security capabilities of the service, Microsoft can stay ahead of emerging threats.

"We don't have the resources to respond to security threats all day, 365 days a year, the way that Microsoft does."

Bo Wandschneider,
CIO and Associate Vice Principal
Queen's University (Canada)

Incident management and response. Microsoft has a global, 24x7 incident response service that works to mitigate the effects of attacks and malicious activity. The incident response team follows established procedures for incident management, communication, and recovery, and uses discoverable and predictable interfaces with internal and external partners alike. In the event of a security incident, the security team follows these five phases:



- **Identification**: If an event indicates a security issue, the incident is assigned a severity classification and appropriately escalated within Microsoft.
- **Containment**: The immediate priority of the escalation team is to ensure the incident is contained and data is safe.
- **Eradication**: After the situation is contained, the escalation team moves toward eradicating any damage caused by the security incident and identifies the root cause of the security issue.
- **Recovery**: Software or configuration updates are applied to the system and services are returned to full working capacity.
- **Lessons Learned**: Each security incident is analyzed to ensure the appropriate mitigations are applied to protect against future recurrence.

Infrastructure Protection

Azure infrastructure includes hardware, software, networks, administrative and operations staff, and the physical data centers that house it all. Azure addresses security risks across its infrastructure.

Physical security. Azure runs in geographically distributed Microsoft facilities, sharing space and utilities with other Microsoft Online Services. Each facility is designed to run 24x7x365 and employs various measures to help protect operations from power failure, physical intrusion, and network outages. These datacenters comply with industry standards (such as ISO 27001) for physical security and availability. They are managed, monitored, and administered by Microsoft operations personnel.

Monitoring and logging. Centralized monitoring, correlation, and analysis systems manage the large amount of information generated by devices within the Azure environment, providing continuous visibility and timely alerts to the teams that manage the service. Additional monitoring, logging, and reporting capabilities provide visibility to customers.

Perimeter	Buildings	Computer room
• Security staff around the clock • Facility setback requirements • Barriers • Fencing	• Alarms • Security operations center • Seismic bracing • Security cameras	• Two-factor access control: biometric and card readers • Cameras • Days of backup power

Update management. Security update management helps protect systems from known vulnerabilities. Azure uses integrated deployment systems to manage the distribution and installation of security updates for Microsoft software. Azure uses a combination of Microsoft and third-party scanning tools to run OS, web application, and database scans of the Azure environment.

Antivirus and antimalware. Azure software components must go through a virus scan prior to deployment. Code is not moved to production without a clean and successful virus scan. In addition, Microsoft provides native antimalware on all Azure VMs. Microsoft recommends that customers run some form of antimalware or antivirus on all virtual machines (VMs). Customers can install Microsoft Antimalware for Cloud Services and Virtual Machines or another antivirus solution on VMs, and VMs can be routinely reimaged to clean out intrusions that may have gone undetected.

Penetration testing. Microsoft conducts regular penetration testing to improve Azure security controls and processes. Microsoft understands that security assessment is also an important part of our customers' application development and deployment. Therefore, Microsoft has established a policy for customers to carry out authorized penetration testing on their own—and only their own—applications hosted in Azure.

DDoS Protection. Azure has a defense system against Distributed Denial-of-Service (DDoS) attacks on Azure platform services. It uses standard detection and mitigation techniques. Azure's DDoS defense system is designed to withstand attacks generated from outside and inside the platform.

Network Protection

Azure networking provides the infrastructure necessary to securely connect VMs to one another and to connect on-premises data centers with Azure VMs. Because Azure's shared infrastructure hosts hundreds of millions of active VMs, protecting the security and confidentiality of network traffic is critical.

In the traditional datacenter model, a company's IT organization controls networked systems, including physical access to networking equipment. In the cloud service model, the responsibilities for network protection and management are shared between the cloud provider and the customer. Customers do not have physical access, but they implement the logical equivalent within their cloud environment through tools such as Guest operating system (OS) firewalls, Virtual Network Gateway configuration, and Virtual Private Networks.

Network isolation. Azure is a multitenant service, meaning that multiple customers' deployments and VMs are stored on the same physical hardware. Azure uses logical isolation to segregate each customer's data from that of others. This provides the scale and economic benefits of multitenant services while rigorously preventing customers from accessing one another's data.

Virtual networks. A customer can assign multiple deployments within a subscription to a virtual network and allow those deployments to communicate with each other through private IP addresses. Each virtual network is isolated from other virtual networks.

VPN and Express Route. Microsoft enables connections from customer sites and remote workers to Azure Virtual Networks using Site-to-Site and Point-to-Site VPNs. For even better performance, customers can use an optional ExpressRoute, a private fiber link into Azure data centers that keeps their traffic off the Internet.

Encrypting communications. Built-in cryptographic technology enables customers to encrypt communications within and between deployments, between Azure regions, and from Azure to on-premises data centers.

"If you're resisting the cloud because of security concerns, you're running out of excuses."

FORRESTER®

Data Protection

Azure allows customers to encrypt data and manage keys, and safeguards customer data for applications, platform, system and storage using three specific methods: encryption, segregation, and destruction.

Data isolation. Azure is a multitenant service, meaning that multiple customers' deployments and virtual machines are stored on the same physical hardware.

Protecting data at rest. Azure offers a wide range of encryption capabilities, giving customers the flexibility to choose the solution that best meets their needs. Azure Key Vault helps customers easily and cost effectively streamline key management and maintain control of keys used by cloud applications and services to encrypt data.

Protecting data in transit. For data in transit, customers can enable encryption for traffic between their own VMs and end users. Azure protects data in transit, such as between two virtual networks. Azure uses industry standard transport protocols such as TLS between devices and Microsoft datacenters, and within datacenters themselves.

Encryption. Customers can encrypt data in storage and in transit to align with best practices for protecting confidentiality and data integrity. For data in transit, Azure uses industry-standard transport protocols between devices and Microsoft datacenters and within datacenters themselves. You can enable encryption for traffic between your own virtual machines and end users.

Data redundancy. Customers may opt for in-country storage for compliance or latency considerations or out-of-country storage for security or disaster recovery purposes. Data may be replicated within a selected geographic area for redundancy.

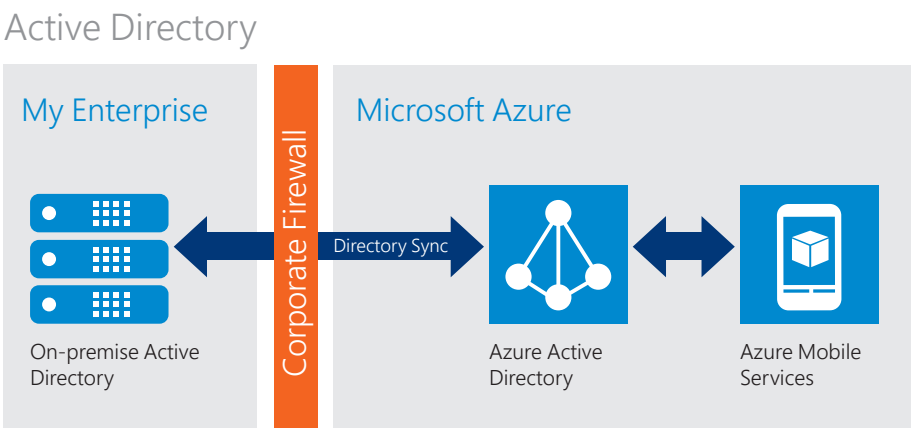
Data destruction. When customers delete data or leave Azure, Microsoft follows strict standards for overwriting storage resources before reuse. As part of our agreements for cloud services such as Azure Storage, Azure VMs, and Azure Active Directory, we contractually commit to specific processes for the deletion of data.

> **"From a security point of view, I think Azure is a demonstrably more secure environment than most banks' datacenters."**
>
> John Schlesinger,
> *Chief Enterprise Architect, Temenos (Switzerland)*

Identity and Access

Microsoft has strict controls that restrict access to Azure by Microsoft employees. Azure also enables customers to control access to their environments, data and applications.

Enterprise cloud directory. Azure Active Directory is a comprehensive identity and access management solution in the cloud. It combines core directory services, advanced identity governance, security, and application access management. Azure Active Directory makes it easy for developers to build policy-based identity management into their applications. Azure Active Directory Premium includes additional features to meet the advanced identity and access needs of enterprise organizations. Azure Active Directory enables a single identity management capability across on-premises, cloud, and mobile solutions.



Multi-Factor Authentication. Microsoft Azure provides Multi-Factor Authentication (MFA). This helps safeguard access to data and applications and enables regulatory compliance while meeting user demand for a simple sign-in process for both on-premises and cloud applications. It delivers strong authentication via a range of easy verification options—phone call, text message, or mobile app notification—allowing users to choose the method they prefer.

Access monitoring and logging. Security reports are used to monitor access patterns and to proactively identify and mitigate potential threats. Microsoft administrative operations, including system access, are logged to provide an audit trail if unauthorized or accidental changes are made. Customers can turn on additional access monitoring functionality in Azure and use third-party monitoring tools to detect additional threats. Customers can request reports from Microsoft that provide information about user access to their environments.

Privacy: Customers own and control their data

Customers will only use cloud providers in which they have great trust. They must trust that the privacy of their information will be protected, and that their data will be used in a way that is consistent with their expectations.

We build privacy protections into Azure through Privacy by Design, a program which describes how we build and operate products and services to protect privacy. Standards and processes that support Privacy by Design principles include the Microsoft Online Services Privacy Statement (which details Microsoft's core privacy requirements and practices) and the Microsoft Secure Development Lifecycle (which includes addressing privacy requirements).

"The question is no longer: 'How do I move to the cloud?' Instead, it's 'Now that I'm in the cloud, how do I make sure I've optimized my investment and risk exposure?'"

We then back those protections with strong contractual commitments to safeguard customer data, including offering EU Model Clauses (which provides terms covering the processing of personal information), and complying with international standards.

Microsoft uses customer data stored in Azure only to provide the service, including purposes compatible with providing the service. Azure does not use customer data for advertising or similar commercial purposes.

Contractual commitments. Microsoft was the first major cloud service provider to make contractual privacy commitments that help assure the privacy protections built into in-scope Azure services are strong. Among the many commitments that Microsoft supports are:

- EU Model Clauses. EU data protection law regulates the transfer of EU customer personal data to countries outside the European Economic Area (EEA). Microsoft offers customers the EU Standard Contractual Clauses that provide specific contractual guarantees around transfers of personal data for in-scope services. Europe's privacy regulators have determined that the contractual privacy protections Azure delivers to its enterprise cloud customers meet current EU standards for international transfers of data. Microsoft is the first cloud provider to receive this recognition.
- US-EU Safe Harbor Framework and the US-Swiss Safe Harbor Program. Microsoft abides by these frameworks set forth by the US Department of Commerce regarding the collection, use, and retention of data from the EEA and Switzerland.
- ISO/IEC 27018. Microsoft is the first major cloud provider to adopt the first international code of practice for cloud privacy. ISO/IEC 27018 was developed to establish a uniform, international approach to protecting the privacy of personal data stored in the cloud. The British Standards Institution independently verified that Microsoft Azure is aligned with the guideline's code of practice. ISO 27018 controls include a prohibition on the use of customer data for advertising and marketing purposes without the customer's express consent

Restricted access by Microsoft personnel. Access to customer data by Microsoft personnel is restricted. Customer data is only accessed when necessary to support the customer's use of Azure. This may include troubleshooting aimed at preventing, detecting, or repairing problems affecting the operation of Azure and the improvement of features that involve the detection of, and protection against, emerging and evolving threats to the user (such as malware or spam). When granted, access is controlled and logged. Strong authentication, including the use of multi-factor authentication, helps limit access to authorized personnel only. Access is revoked as soon as it is no longer needed.

Notification of lawful requests for information. Microsoft believes that customers should control their data whether stored on their premises or in a cloud service. We will not disclose Azure customer data to law enforcement except as a customer directs or where required by law. When governments make a lawful demand for Azure customer data from Microsoft, we strive to be principled, limited in what we disclose, and committed to transparency.

- Microsoft does not provide any third party with direct or unfettered access to customer data. Microsoft only releases specific data mandated by the relevant legal demand.
- If a government wants customer data—including for national security purposes—it needs to follow the applicable legal process, meaning it must serve us with a warrant or court order for content or subpoena for account information. If compelled to disclose customer data, we will promptly notify the customer and provide a copy of the demand unless legally prohibited from doing so.

- Microsoft will only respond to requests for specific accounts and identifiers. There is no blanket or indiscriminate access to Microsoft's customer data. Every request is explicitly reviewed by Microsoft's legal team, who ensures that the requests are valid, rejects those that are not, and makes sure we only provide the data specified in the order.

In its commitment to transparency, Microsoft regularly publishes a Law Enforcement Requests Report that discloses the scope and number of requests we receive.

Greater transparency and simplicity of data use policies.
Microsoft keeps customers informed about the processes to protect data privacy and security, including practices and policies. Microsoft also provides the summaries of independent audits of services, which helps customers pursue their own compliance.

Customers are in control of their data

For many organizations, the benefits of moving to the cloud are clear. Still, fear of losing control causes their decision makers to hesitate. Where will data be stored? Who owns the organization's data? Who will be accessing the data? And what happens if the organization wants to switch providers? These are all valid questions—questions Microsoft has in mind when making a clear commitment to provide customers with control over their data. This commitment is unique among major cloud service providers.

Customers own their data. This belief is fundamental to the Microsoft approach. When a customer utilizes Azure, they retain exclusive ownership of their data. Microsoft takes steps to protect many types of data.

Microsoft defines customer data as "all data, including all text, sound, video or image files, and software that are provided to Microsoft by, or on behalf of, Customer through use of the Online Service." For example, this includes data that you upload for storage or processing and applications that you run in Azure.

Customers can access their own customer data at any at any time and for any reason without assistance from Microsoft. Microsoft will not use customer data or derive information from it for advertising. We will use customer data only to provide the service or for purposes compatible with providing the service.

"Just as computer users back up their laptops in case they break or are lost, Estonia is working out how to back up the country, in case it is attacked by Russia."

The Economist,
reporting on Estonia's Azure cloud backup

- **Customer data** is all data, including all text, sound, video or image files, and software that are provided to Microsoft by or on behalf of the customer through use of Azure. For example, it includes data uploaded for storage or processing and applications uploaded by the customer for hosting on Azure.
- **Administrator data** is the information about administrators (including account contact and subscription administrators) supplied during signup, purchase, or administration of Azure, such as name, phone number, and email address.
- **Metadata** includes configuration and technical settings and information. For example, it includes the disk configuration settings for an Azure virtual machine or the database design for an SQL Database. Metadata does not include information from which customer data could be derived.
- **Access control data** is data that is used to manage access to other types of data or functions within Azure. It includes passwords, security certificates, and other authentication-related data.

Control over data location. When customers entrust their data to Microsoft, they are not giving up control. For many customers, knowing and controlling the location of their data can be an important element of data privacy, compliance, and governance. Microsoft Azure offers an ever-expanding network of data centers across the globe. Most Azure services permit customers to specify the particular geography where their customer data will be stored. Data may be replicated within a selected geographic area for redundancy, but will not be replicated outside it for redundancy.

Encryption key management. To ensure control over encrypted data, customers have the option to generate and manage their own encryption keys, and determine who is authorized to use them. They also have the option to revoke Microsoft's copy of their encryption key, although this may limit Microsoft's ability to troubleshoot or repair problems and security threats.

Role based access control. Microsoft provides an approach allowing customers to restrict system access to authorized users based on role assignment, role authorization, and permission authorization. Tools in multiple Microsoft cloud services support authorization based on a user's role, simplifying access control across defined groups of users.

Control over data destruction. When customers delete data or leave a Microsoft cloud service, Microsoft follows strict standards for overwriting storage resources before reuse, as well physical destruction of decommissioned hardware, including contractual commitments to specific processes for the deletion of data and the destruction of storage hardware.

"Our brand rests on the continuity of our IT systems, which are now more available running in Azure."

Andrew Goodin,
Global Manager of Information Systems
Zespri International (New Zealand)

Transparency

For customers to effectively exercise their right to control their data, they must have access and visibility to that data. They must know where it is stored. They must also know, through clearly stated and readily available policies and procedures, how the cloud provider helps secure customer data, who can access it, and under what circumstances.

Where and how data is stored and used. Microsoft gives Azure customers visibility to where their customer data is stored in an ever-expanding network of datacenters around the globe. Customers can balance the need to store backups at multiple locations in case of a disaster with the need to keep their data out of certain geographies. Microsoft provides clear data maps and geographic boundary information for all datacenters.

How data is secured. Customers have access to up-to-date information regarding security policies and procedures. Microsoft promotes transparency by publishing and adhering to the Security Development Lifecycle.

Who requests access to customer data. Microsoft will never disclose Azure customer data to a government or law enforcement agency except as directed by the customer or where required by law. In response to lawful demands for Azure customer data, Microsoft strives to be principled, limited in disclosure, and committed to transparency. Microsoft regularly publishes a Law Enforcement Requests Report that discloses the scope and number of government requests received.

Breach notification. In the event that customer data is compromised, Microsoft will notify its customers. Azure has comprehensive, transparent policies that govern incident response from identification all the way through to lessons learned.

Audit standards certifications. Rigorous third-party audits, such as those conducted by the British Standards Institute, verify Azure's adherence to the strict security controls these standards mandate. As part of Microsoft's commitment to transparency, customers can verify Azure's implementation of many security controls by requesting audit results from the certifying third parties.

Customer guidance. Microsoft publishes a Security Response Center Progress Report and a Security Intelligence Report to provide customers with insights into the threat landscape, and provide prescriptive guidance for managing risk to protect their assets.

Transparency Centers. Microsoft operates Transparency Centers that provide government customers with the ability to review source code, reassure themselves of its integrity, and confirm there are no back doors.

"By 2020 clouds will stop being referred to as 'public' and 'private'. It will simply be the way business is done and IT is provisioned."

Compliance: Azure conforms to global standards

Microsoft invests heavily in the development of robust and innovative compliance processes. The Microsoft compliance framework for online services maps controls to multiple regulatory standards. This enables Microsoft to design and build services using a common set of controls, streamlining compliance across a range of regulations today and as they evolve in the future.

Microsoft compliance processes also make it easier for customers to achieve compliance across multiple services and meet their changing needs efficiently. Together, security-enhanced technology and effective compliance processes enable Microsoft to maintain and expand a rich set of third-party certifications. These help customers demonstrate compliance readiness to their customers, auditors, and regulators. As part of its commitment to transparency, Microsoft shares third-party verification results with its customers.

Certifications and attestations. Azure meets a broad set of international as well as regional and industry-specific compliance standards, such as ISO 27001, FedRAMP, SOC 1 and SOC 2. Azure's adherence to the strict security controls contained in these standards is verified by rigorous third-party audits that demonstrate Azure services work with and meet world-class industry standards, certifications, attestations, and authorizations.

Comprehensive, independently verified compliance. Azure is designed with a compliance strategy that helps customers address business objectives and industry standards and regulations. The security compliance framework includes test and audit phases, security analytics, risk management best practices, and security benchmark analysis to achieve certificates and attestations. Microsoft Azure offers the following certifications for all in-scope services.

CDSA. The Content Delivery and Security Association (CDSA) provides a Content Protection and Security (CPS) standard for compliance with anti-piracy procedures governing digital media. Azure passed the CDSA audit, enabling secure workflows for content development and distribution.

CJIS. Any US state or local agency that wants to access the FBI's Criminal Justice Information Services (CJIS) database is required to adhere to the CJIS Security Policy. Azure is the only major cloud provider that contractually commits to conformance with the CJIS Security Policy, which commits Microsoft to adhere to the same requirements that law enforcement and public safety entities must meet.

CSA CCM. The Cloud Security Alliance (CSA) is a nonprofit, member-driven organization with a mission to promote the use of best practices for providing security assurance within the cloud. The CSA Cloud Controls Matrix (CCM) provides detailed information about how Azure fulfills the security, privacy, compliance, and risk management requirements defined in the CCM version 1.2, and is published in the CSA's Security Trust and Assurance Registry (STAR).

EU Model Clauses. Microsoft offers customers EU Standard Contractual Clauses that provide contractual guarantees around transfers of personal data outside of the EU. Microsoft is the first company to receive joint approval from the EU's Article 29 Working Party that the contractual privacy protections Azure delivers to its enterprise cloud customers meet current EU standards for international transfers of data. This ensures that Azure customers can use Microsoft services to move data freely through our cloud from Europe to the rest of the world.

FDA 21 CFR Part 11. The US Food and Drug Administration (FDA) Code of Federal Regulations (CFR) Title 21 Part 11 lists requirements for the security of electronic records of companies that sell food and drugs manufactured or consumed in the United States. The compliance reports produced by Azure's independent third party SSAE and ISO auditors identify the procedural and technical controls established at Microsoft and can be used to satisfy the requirements of CFR Title 21 Part 11. Microsoft is able to show how relevant controls within these reports have an impact on compliance with the FDA 21 CFR 11 regulations.

FedRAMP. Azure has been granted a Provisional Authority to Operate (P-ATO) from the Federal Risk and Authorization Management Program (FedRAMP) Joint Authorization Board (JAB) at a Moderate impact level based upon the FIPS 199 classification. FedRAMP is a US government program that provides a standard approach to security assessment, authorization, and monitoring for cloud services used by federal agencies and thereby saves the taxpayer and individual organizations the time and cost of conducting their own independent reviews.

FERPA. The Family Educational Rights and Privacy Act (FERPA) is a US federal law that protects the privacy of student educational records. Microsoft agrees to use and disclosure restrictions imposed by FERPA.

FIPS 140-2. Azure complies with the Federal Information Processing Standard (FIPS) Publication 140-2, a US government standard that defines a minimum set of security requirements for products and systems that implement cryptography.

HIPAA. The Health Insurance Portability and Accountability Act (HIPAA) is a US federal law that regulates patient Protected Health Information (PHI). Azure offers customers a HIPAA Business Associate Agreement (BAA), stipulating adherence to certain security and privacy provisions in HIPAA and the HITECH Act. To assist customers in their individual compliance efforts, Microsoft offers a BAA to Azure customers as a contract addendum.

IRAP. Azure has been assessed against the Australian Government Information Security Registered Assessors Program (IRAP), which provides assurance for public sector customers that Microsoft has appropriate and effective security controls.

ISO/IEC 27018. Microsoft is the first cloud provider to have adopted the ISO/IEC 27018 code of practice, covering the processing of personal information by cloud service providers.

ISO/IEC 27001/27002:2013. Azure complies with this standard, which defines the security controls required of an information security management system.

MLPS. Multi-Level Protection Scheme (MLPS) is based on the Chinese state standard issued by the Ministry of Public Security. Azure operated by 21Vianet adheres to this standard, which provides assurance for both the management and technical security of cloud systems.

MTCS. Azure has achieved Level-1 certification with the Multi-Tier Cloud Security Standard for Singapore (MTCS SS), a cloud security standard covering areas such as data security, confidentiality, business impact, and operational transparency, developed under the Singapore Information Technology Standards Committee.

PCI DSS. Azure is Level 1 compliant with Payment Card Industry (PCI) Data Security Standards (DSS) version 3.0, the global certification standard for organizations that accept most payments cards, as well store, process, or transmit cardholder data.

SOC 1 and SOC 2. Azure has been audited against the Service Organization Control (SOC) reporting framework for both SOC 1 Type 2 and SOC 2 Type 2. Both reports are available to customers to meet a wide range of US and international auditing requirements.

The SOC 1 Type 2 audit report attests to the design and operating effectiveness of Azure controls. The SOC 2 Type 2 audit included a further examination of Azure controls related to security, availability, and confidentiality. Azure is audited annually to ensure that security controls are maintained.

TCS CCCPPF. Azure operated by 21Vianet is among the first cloud providers in China to pass the Trusted Cloud Service certification developed by the China Cloud Computing Promotion and Policy Forum (CCCPPF).

UK G-Cloud. The UK Government G-Cloud is a cloud computing certification for services used by government entities in the United Kingdom. Azure has received OFFICIAL accreditation from the UK Government Pan Government Accreditor.

Additional resources

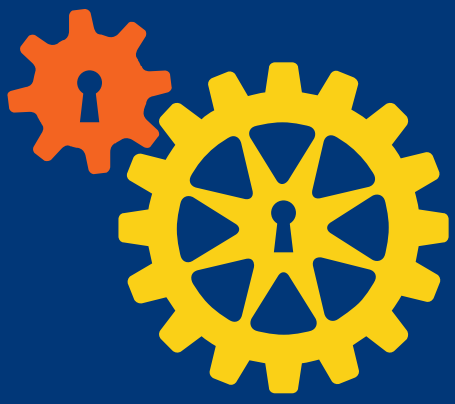
Azure Trust Center
http://azure.microsoft.com/trustcenter

Cloud Security Alliance Cloud Controls Matrix
https://cloudsecurityalliance.org/research/ccm/

Microsoft Cloud Security Readiness Tool
http://www.microsoft.com/trustedcloud

Microsoft Online Services Privacy Statement
http://aka.ms/onlineservices-privacy

Microsoft Privacy Practices
http://aka.ms/privacy-practices



NOTE: Certain recommendations contained herein may result in increased data, network, or compute resource usage, and increase your license or subscription costs.

Disaster Recovery and High Availability for Azure Applications

Updated: February 23, 2015
Primary Authors: Michael McKeown, Cloud Solutions Architect (Aditi); Hanu Kommalapati, Principal Technology Evangelist (Microsoft)
Contributing Author: Jason Roth
Reviewers: Patrick Wickline, Dennis Mulder, Steve Howard, Tim Wieman, James Podgorski, Ryan Berry, Shweta Gupta, Harry Chen, Jim Blanchard, Andy Roberts, Christian Els

Introduction

This paper focuses on high availability for applications running in Azure. An overall strategy for high availability also includes the area of disaster recovery (DR). Planning for failures and disasters in the cloud requires you to recognize the failures quickly. You then implement a strategy that matches your tolerance for the application's downtime. Additionally, you have to consider the extent of data loss the application can tolerate without causing adverse business consequences as it is restored.

When we ask customers if they are prepared for temporary and large-scale failures, most say they are. However, before you answer that question for yourself, does your company rehearse these failures? Do you test the recovery of databases to ensure you have the correct processes in place? Chances are probably not. That's because successful DR starts with lots of planning and architecting to implement these processes. Just like many other non-functional requirements, such as security, disaster recovery rarely gets the up-front analysis and time allocation it requires. Also, most customers don't have the budget for geographically distributed datacenters with redundant capacity. Consequently, even mission critical applications are frequently excluded from proper DR planning.

Cloud platforms, such as Azure, provide geographically dispersed datacenters around the world. These platforms also provide capabilities that support availability and a variety of DR scenarios. Now, every mission critical cloud application can be given due consideration for disaster proofing of the system. Azure has resiliency and DR built in to many of its services. You must study these platform features carefully and supplement with application strategies.

This whitepaper outlines the necessary architecture steps you must take to disaster-proof an Azure deployment. Then you can implement the larger business continuity process. A business continuity plan is a roadmap for continuing operations under adverse conditions. This could be a failure with technology, such as a downed service, or a natural disaster, such as a storm or power outage. Application resiliency for disasters is only a subset of the larger DR process as described in this NIST document: Contingency Planning Guide for Information Technology Systems.

The following sections define different levels of failures, techniques to deal with them, and architectures that support these techniques. This information provides input to your DR processes and procedures to ensure your DR strategy works correctly and efficiently.

Characteristics of Resilient Cloud Applications

A well architected application can withstand capability failures at a tactical level and can also tolerate strategic system-wide failures at the datacenter level. The following sections define the terminology referenced throughout the document to describe various aspects of resilient cloud services.

High Availability

A highly available cloud application implements strategies to absorb the outage of the dependencies like the managed services offered by the cloud platform. Despite possible failures of the cloud platform's capabilities, this

approach permits the application to continue to exhibit the expected functional and non-functional systemic characteristics. This is covered in depth in the paper Failsafe: Guidance for Resilient Cloud Architectures.
When you implement the application, you must consider the probability of a capability outage. Additionally, consider the impact an outage will have on the application from the business perspective before diving deep into the implementation strategies. Without due consideration to the business impact and the probability of hitting the risk condition, the implementation can be expensive and potentially unnecessary.
Consider an automotive analogy for high availability. Even quality parts and superior engineering does not prevent occasional failures. For example, when your car gets a flat tire, the car still runs, but it is operating with degraded functionality. If you planned for this potential occurrence, you can use one of those thin-rimmed spare tires until you reach a repair shop. Although the spare tire does not permit fast speeds, you can still operate the vehicle until you replace the tire. Similarly, a cloud service that plans for potential loss of capabilities can prevent a relatively minor problem from bringing down the entire application. This is true even if the cloud service must run with degraded functionality.
There are a few key characteristics of highly available cloud services: availability, scalability, and fault tolerance. Although these characteristics are interrelated, it is important to understand each and how they contribute to the overall availability of the solution.

Availability

An available application considers the availability of its underlying infrastructure and dependent services. Available applications remove single points of failure through redundancy and resilient design. When we talk about availability in Azure, it is important to understand the concept of the *effective availability* of the platform. Effective availability considers the Service Level Agreements (SLA) of each dependent service and their cumulative effect on the total system availability.
System availability is the measure of the percentage of a time window the system will be able to operate. For example, the availability SLA of at least two instances of a web or worker role in Azure is 99.95% (out of 100%). It does not measure the performance or functionality of the services running on those roles. However, the effective availability of your cloud service is also affected by the various SLA of the other dependent services. The more moving parts within the system, the more care you must take to ensure the application can resiliently meet the availability requirements of its end users.
Consider the following SLAs for an Azure service that uses Azure services: Compute, Azure SQL Database, and Azure Storage.

Azure Service	SLA	Potential Minutes Downtime/Month (30 days)
Compute	99.95%	21.6
SQL Database	99.90%	43.2
Storage	99.90%	43.2

You must plan for all services to potentially go down at different times. In this simplified example, the total number of minutes per month that the application could be down is 108 minutes. A 30-day month has a total of 43,200 minutes. 108 minutes is .25% of the total number of minutes in a 30-day month (43,200 minutes). This gives you an effective availability of 99.75% for the cloud service.
However, using availability techniques described in this paper can improve this. For example, if you design your application to continue running when the SQL Database is unavailable, you can remove that from the equation. This might mean that the application runs with reduced capabilities, so there are also business requirements to consider. For a complete list of Azure SLA's, see Service Level Agreements.

Scalability

Scalability directly affects availability—an application that fails under increased load is no longer available. Scalable applications are able to meet increased demand with consistent results in acceptable time windows. When a system is scalable, it scales horizontally or vertically to manage increases in load while maintaining consistent performance. In basic terms, horizontal scaling adds more machines of the same size (processor, memory, bandwidth) while vertical scaling increases the size of the existing machines. For Azure, you have vertical scaling options for selecting various machine sizes for compute. However, changing the machine size requires a re-deployment. Therefore, the most flexible solutions are designed for horizontal scaling. This is especially true for compute because you can easily increase the number of running instances of any web or worker role. These additional instances handle increased traffic through the Azure Web portal, PowerShell scripts, or code. Base this decision on increases in specific monitored metrics. In this scenario, user performance or metrics do not suffer a noticeable drop under load. Typically, the web and worker roles store any state externally. This allows for flexible load balancing and graceful handling of any changes to instance counts. Horizontal scaling also works well with services, such as Azure Storage, which do not provide tiered options for vertical scaling.

Cloud deployments should be seen as a collection of scale-units. This allows the application to be elastic in servicing the throughput needs of end users. The scale units are easier to visualize at the web and application server level. This is because Azure already provides stateless compute nodes through web and worker roles. Adding more compute scale-units to the deployment will not cause any application state management side effects because compute scale-units are stateless. A storage scale-unit is responsible for managing a partition of data (structured or unstructured). Examples of storage scale-units include Azure Table partition, Blob container, and SQL Database. Even the usage of multiple Azure Storage accounts has a direct impact on the application scalability. You must design a highly scalable cloud service to incorporate multiple storage scale-units. For instance, if an application uses relational data, partition the data across several SQL Databases. Doing so allows the storage to keep up with the elastic compute scale-unit model. Similarly, Azure Storage allows data partitioning schemes that require deliberate designs to meet the throughput needs of the compute layer. For a list of best practices for designing scalable cloud services, see Best Practices for the Design of Large-Scale Services on Azure Cloud Services.

Fault Tolerance

Applications need to assume that every dependent cloud capability can and will go down at some point in time. A fault tolerant application detects and maneuvers around failed elements to continue and return the correct results within a specific timeframe. For transient error conditions, a fault tolerant system will employ a retry policy. For more serious faults, the application can detect problems and fail over to alternative hardware or contingency plans until the failure is corrected. A reliable application can properly manage the failure of one or more parts and continue operating properly. Fault tolerant applications can use one or more design strategies, such as redundancy, replication, or degraded functionality.

Disaster Recovery

A cloud deployment might cease to function due to a systemic outage of the dependent services or the underlying infrastructure. Under such conditions, a business continuity plan triggers the disaster recovery (DR) process. This process typically involves both operations personnel and automated procedures in order to reactivate the application at a functioning datacenter. This requires the transfer of application users, data, and services to the new datacenter. It also involves the use of backup media or ongoing replication.

Consider the previous analogy that compared high availability to the ability to recover from a flat tire through the use of a spare. In contrast, disaster recovery involves the steps taken after a car crash where the car is no longer operational. In that case, the best solution is to find an efficient way to change cars by calling a travel service or a friend. In this scenario, there is likely going to be a longer delay in getting back on the road. There is also more complexity in repairing and returning to the original vehicle. In the same way, disaster recovery to another datacenter is a complex task that typically involves some downtime and potential loss of data. To better understand and evaluate disaster recovery strategies, it is important to define two terms: recovery time objective (RTO) and recovery point objective (RPO).

RTO

The recovery time objective (RTO) is the maximum amount of time allocated for restoring application functionality. This is based on business requirements and is related to the importance of the application. Critical business applications require a low RTO.

RPO

The recovery point objective (RPO) is the acceptable time window of lost data due to the recovery process. For example, if the RPO is one hour, you must completely back up or replicate the data at least every hour. Once you bring up the application in an alternate datacenter, the backup data may be missing up to an hour of data. Like RTO, critical applications target a much smaller RPO.

Part 1: High Availability

A highly available application absorbs fluctuations in availability, load, and temporary failures in the dependent services and hardware. The application continues to operate at an acceptable user and systemic response level as defined by business requirements or application service level agreements.

Azure High Availability Features

Azure has many built-in platform features that support highly available applications. This section describes some of those key features. For a more comprehensive analysis of the platform, see Azure Business Continuity Technical Guidance.

The Azure Fabric Controller (FC) is responsible for provisioning and monitoring the condition of the Azure compute instances. The Fabric Controller checks the status of the hardware and software of the host and guest machine instances. When it detects a failure, it enforces SLAs by automatically relocating the VM instances. The concept of fault and upgrade domains further supports the compute SLA.

When multiple role instances are deployed, Azure deploys these instances to different fault domains. A fault domain boundary is basically a different hardware rack in the same datacenter. Fault domains reduce the probability that a localized hardware failure will interrupt the service of an application. You cannot manage the number of fault domains that are allocated to your worker or web roles. The Fabric Controller uses dedicated resources that are separate from Azure hosted applications. It has 100% uptime because it serves as the nucleus of the Azure system. It monitors and manages role instances across fault domains. The following diagram shows Azure shared resources that are deployed and managed by the FC across different fault domains.

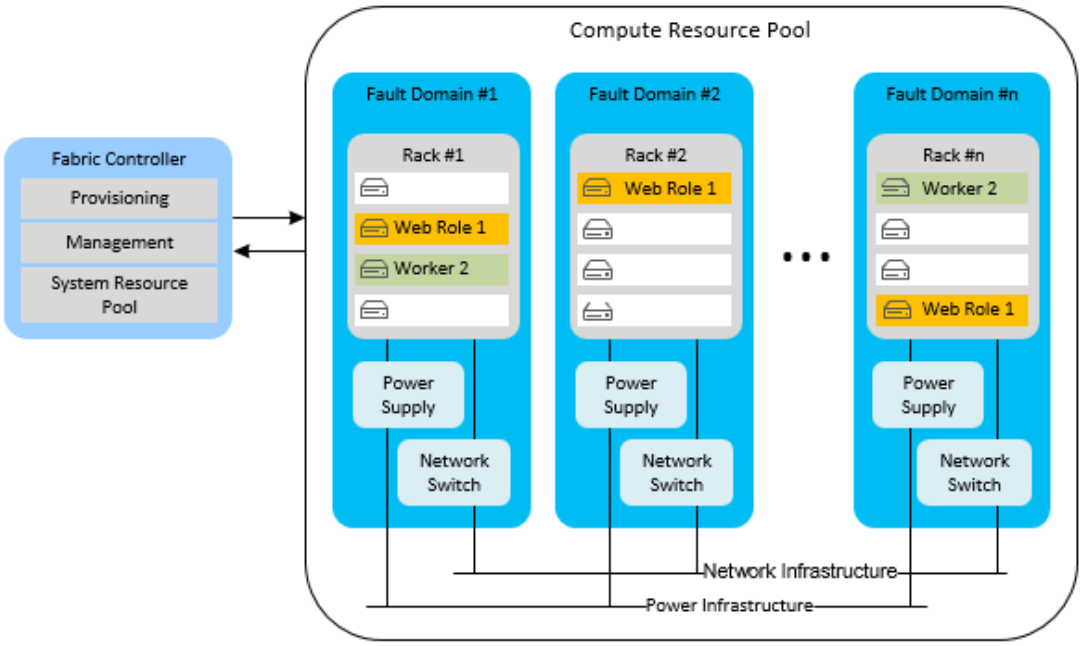


Figure 1 Fault Domain Isolation (Simplified View)

Upgrade domains are similar to fault domains in function, but they support upgrades rather than failures. An upgrade domain is a logical unit of instance separation that determines which instances in a particular service will be upgraded at a point in time. By default, for your hosted service deployment, five upgrade domains are defined. However, you can change that value in the service definition file. For example, you have eight instances of your web role. There will be two instances in three upgrade domains and two instances in one upgrade domain. Azure defines the update sequence, but it is based on the number of upgrade domains. For more information on upgrade domains, see Update an Azure Service.

In addition to these platform features that support high compute availability, Azure embeds high availability features into its other services. For example, Azure Storage maintains three replicas of all blob, table, and queue data. It also allows the option of geo-replication to store backups of blobs and tables in a secondary datacenter. The Content Delivery Network (CDN) allows blobs to be cached around the world for both redundancy and scalability. Azure SQL Database maintains multiple replicas as well. In addition to the Azure Business Continuity Technical Guidance paper, see the Best Practices for the Design of Large-Scale Services on Azure Cloud Services paper. They provide a full discussion of the platform availability features.

Although Azure provides multiple features that support high availability, it is important to understand their limitations. For compute, Azure guarantees that your roles are available and running, but it does not know if your application is running or overloaded. For Azure SQL Database, data is replicated synchronously within the datacenter. These database replicas are not point-in-time backups. For Azure Storage, table and blob data is replicated by default to an alternate datacenter. However, you cannot access the replicas until Microsoft chooses to fail over to the alternate site. A datacenter failover typically only occurs in the case of a prolonged datacenter-wide outage, and there is no SLA for geo-failover time. It is also important to note that any data corruption quickly spreads to the replicas. For these reasons, you must supplement the platform availability features with application-specific availability features. These application availability features include the blob snapshot feature to create point-in-time backups of blob data.

The majority of this paper focuses on cloud services, which use a Platform as a Service (PaaS) model. However, there are also specific availability features for Azure Virtual Machines, which use an Infrastructure as a Service (IaaS) model. In order to achieve high availability with Virtual Machines, you must use availability sets. An availability set serves a similar function to fault and upgrade domains. Within an availability set, Azure positions the virtual machines in a way that prevents localized hardware faults and maintenance activities from bringing down all of the machines in that group. Availability sets are required to achieve the Azure SLA for the availability of Virtual Machines. The following diagram provides a representation of two availability sets that group web and SQL Server virtual machines respectively.

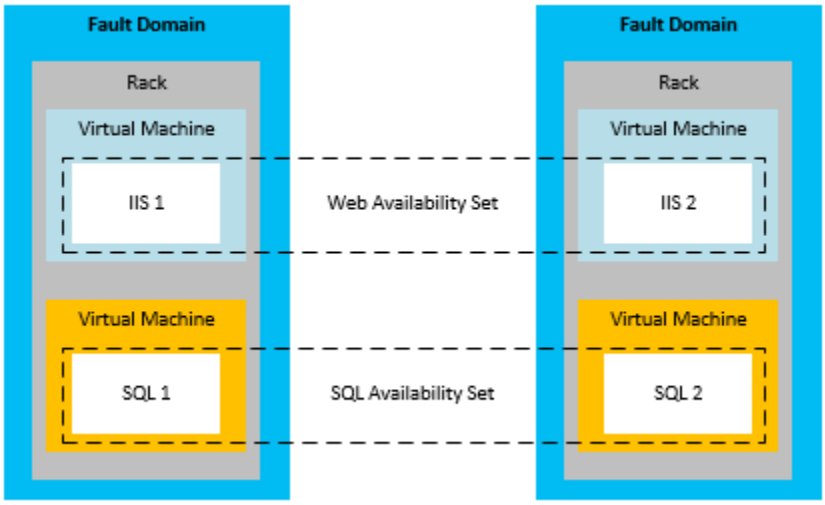


Figure 2 Availability Sets for Azure Virtual Machines

Note that in the previous diagram, SQL Server is installed and running on virtual machines. This is different from the previous discussion of Azure SQL Database, which provides database as a managed service.

Application Strategies for High Availability

Most application strategies for high availability involve either redundancy or the removal of hard dependencies between application components. Application design should support fault tolerance during sporadic downtime of Azure or third-party services. The following sections describe several application patterns for increasing availability of your cloud services.

Asynchronous Communication and Durable Queues

Consider asynchronous communication between loosely-coupled services to increase availability in Azure applications. In this pattern, write messages to either storage queues or Service Bus queues for later processing. When you write the message to the queue, control immediately returns to the sender of the message. Another tier of the application handles the message processing, typically implemented as a worker role. If the worker role goes down, the messages accumulate in the queue until the processing service is restored. As long as the queue is available, there is no direct dependency between the front-end sender and the message processor. This eliminates the requirement for synchronous service calls that can be a throughput bottleneck in distributed applications.

A variation of this uses Azure Storage (blobs, tables, queues) or Service Bus queues as a failover location for failed database calls. For example, a synchronous call within an application to another service (such as Azure SQL Database) fails repeatedly. You may be able to serialize that data into durable storage. At some later point when the service or database is back on-line, the application can re-submit the request from storage. The difference in this model is that the intermediate location is not a constant part of the application workflow. It is used only in failure scenarios.

In both scenarios, asynchronous communication and intermediate storage prevents a downed backend service from bringing the entire application down. Queues serve as a logical intermediary. For more guidance on choosing the correct queuing service, see Azure Queues and Azure Service Bus Queues - Compared and Contrasted.

Fault Detection and Retry Logic

A key point in highly available application design is to utilize retry logic within code to gracefully handle a service that is temporarily down. The The Transient Fault Handling Application Block, developed by the Microsoft Patterns and Practices team, assists application developers in this process. The word “transient” means a temporary condition lasting only for a relatively short time. In the context of this paper, handling transient failures is part of developing a highly available application. Examples of transient conditions include intermittent network errors and lost database connections.

The Transient Fault Handling Application Block is a simplified way for you to handle failures within your code in a graceful manner. It allows you to improve the availability of your applications by adding robust transient fault handling logic. In most cases, retry logic handles the brief interruption and reconnects the sender and receiver after one or more failed attempts. A successful retry attempt typically goes unnoticed to application users.

There are three options for developers to manage their retry logic: incremental, fixed interval, and exponential. Incremental waits longer before each retry in an increasing linear fashion (for example, 1, 2, 3, and 4 seconds). Fixed interval waits the same amount of time between each retry (for example, 2 seconds). For a more random option, the exponential back-off waits longer between retries. However, it uses exponential behavior (for example, 2, 4, 8, and 16 seconds).

The high-level strategy within your code is:

1. Define your retry strategy and policy
2. Try the operation that could result in a transient fault
3. If transient fault occurs, invoke the retry policy

4. If all retries fail, catch a final exception

Test your retry logic in simulated failures to ensure that retries on successive operations do not result in an unanticipated lengthy delay. Do this before deciding to fail the overall task.

Reference Data Pattern (High Availability)

Reference data is the read-only data of an application. This data provides the business context within which the application generates transactional data during the course of a business operation. Transactional data is a point-in-time function of the reference data. Therefore, its integrity depends on the snapshot of the reference data at the time of the transaction. This is a somewhat loose definition, but should suffice for our purpose here.
Reference data in the context of an application is necessary for the functioning of the application. The respective applications create and maintain reference data; Master Data Management systems often perform this function. These systems are responsible for the lifecycle of the reference data. Examples of reference data include product catalog, employee master, parts master, and equipment master. Reference data can also originate from outside the organization, for example, zip codes or tax rates. Strategies for increasing the availability of reference data are typically less difficult than those for transactional data. Reference data has the advantage of being mostly immutable.
You can make Azure web and worker roles that consume reference data autonomous at run time by deploying the reference data along with the application. If the size of the local storage allows such a deployment, this is an ideal state. Embedded databases (SQL, NOSQL) or XML files deployed to a local file system will help with the autonomy of Azure compute scale-units. However, you should have a mechanism to update the data in each role without requiring redeployment. To do this, place any updates to the reference data to a cloud storage endpoint (for example, Azure Blob storage or SQL Database). Add code to each role that downloads the data updates into the compute nodes at role startup. Alternatively, add code that allows an administrator to perform a forced download into the role instances. To increase availability, the roles should also contain a set of reference data in case storage is down. This enables the roles to start with a basic set of reference data until the storage resource becomes available for the updates.

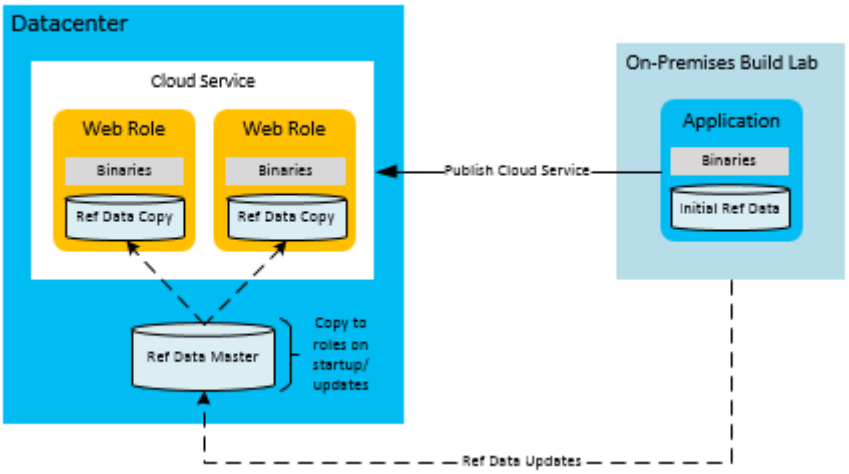


Figure 3 Application high availability through autonomous compute nodes

One consideration for this pattern is the deployment and startup speed for your roles. If you are deploying or downloading large amounts of reference data on startup, this can increase the amount of time it takes to spin up new deployments or role instances. This might be an acceptable tradeoff for the autonomy of having the reference data immediately available on each role rather than depending on external storage services.

Transactional Data Pattern (High Availability)

Transactional data is the data generated by the application in a business context. Transactional data is a combination of the set of business processes the application implements and the reference data that supports these processes. Transactional data examples can include orders, advanced shipping notices, invoices, and CRM

opportunities. The transactional data thus generated will be fed to external systems for record keeping or for further processing.
Keep in mind that reference data can change within the systems that are responsible for this data. For this reason, transactional data must save the point-in-time reference data context so that it has minimal external dependencies for its semantic consistency. For example, consider the removal of a product from the catalog a few months after an order was fulfilled. The best practice is to embed as much reference data context as feasible into the transaction. This preserves the semantics associated with the transaction even if the reference data were to change after the transaction is captured.
As mentioned previously, architectures that use loose coupling and asynchronous communication lend themselves to higher levels of availability. This holds true for transactional data as well, but the implementation is more complex. Traditional transactional notions typically rely on the database for guaranteeing the transaction. When you introduce intermediate layers, the application code must correctly handle the data at various layers to ensure sufficient consistency and durability.
The following sequence describes a workflow that separates the capture of transactional data from its processing:

1. Web Compute Node: Present reference data.
2. External Storage: Save intermediate transactional data.
3. Web Compute Node: Complete the end-user transaction.
4. Web Compute Node: Send the completed transactional data along with the reference data context to a temporary durable storage that is guaranteed to give predictable response.
5. Web Compute Node: Signal end user the completion of the transaction.
6. Background Compute Node: Extract the transactional data, post processes it if necessary, and send it to its final storage location in the current system.

The following diagram shows one possible implementation of this design in an Azure cloud service.

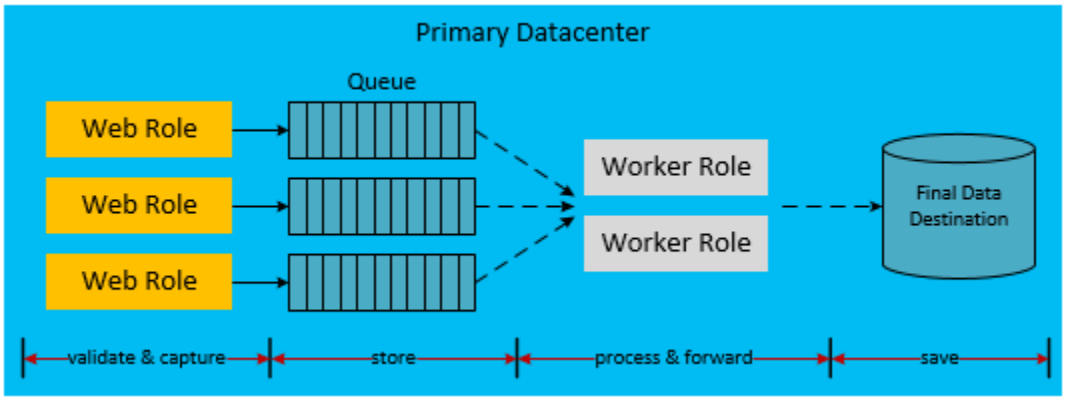


Figure 4 Application high availability through loose coupling

The dashed arrows in the above diagram indicate asynchronous processing. The front-end web role is not aware of this asynchronous processing. This leads to the storage of the transaction at its final destination with reference to the current system. Due to the latency introduced by this asynchronous model, the transactional data is not immediately available for query. Therefore, each unit of the transactional data needs to be saved in a cache or user session to meet the immediate UI needs.
Consequently, the web role is autonomous from the rest of the infrastructure. Its availability profile is a combination of the web role and the Azure queue and not the entire infrastructure. In addition to high availability, this approach allows the web role to scale horizontally, independent of the backend storage. This high availability model can have an impact on the economics of operations. Additional components like Azure queues and worker roles can impact monthly usage costs.

Note that the previous diagram shows one implementation of this decoupled approach to transactional data. There are many other possible implementations. The following list provides some alternative variations.

- A worker role might be placed between the web role and the storage queue.
- A Service Bus queue can be used instead of an Azure Storage queue.
- The final destination might be Azure Storage or a different database provider.
- Azure Caching can be used at the web layer to provide the immediate caching requirements following the transaction.

Scalability Patterns

In addition to the patterns discussed in this section, it is important to note that the scalability of the cloud service directly impacts availability. If increased load causes your service to be unresponsive, the user impression is that the application is down. Follow best practices for scalability based on your expected application load and future expectations. The highest scale involves many considerations, such as the use of single vs. multiple storage accounts, sharing across multiple databases, and caching strategies. For an in-depth look at these patterns, see Best Practices for the Design of Large-Scale Services on Azure Cloud Services.

Part 2: Disaster Recovery

While high availability is about temporary failure management, disaster recovery (DR) is about the catastrophic loss of application functionality. For example, consider the scenario where one or more datacenters go down. In this case, you need to have a plan to run your application or access your data outside of the datacenter. Execution of this plan involves people, processes, and supporting applications that allow the system to function. The business and technology owners, who define its disaster operational mode, determine the level of functionality for the service during a disaster. This can take many forms: completely unavailable, partially available (degraded functionality or delayed processing), or fully available.

Azure Disaster Recovery Features

As with availability considerations, Azure has Azure Business Continuity Technical Guidance designed to support disaster recovery. There is also a relationship between some of the availability features of Azure and disaster recovery. For example, the management of roles across fault domains increases the availability of an application. Without that management, an unhandled hardware failure would become a “disaster” scenario. So the correct application of many of the availability features and strategies should be seen as an important part of disaster-proofing your application. However, this section goes beyond general availability issues to more serious (and rarer) disaster events.

Multiple Datacenter Regions

Azure maintains datacenters in many different regions around the world. This supports several disaster recovery scenarios, such as the system-provided geo-replication of Azure Storage to secondary datacenters. It also means that you can easily and inexpensively deploy a cloud service to multiple locations around the world. Compare this with the cost and difficulty of running your own datacenters in multiple regions. Deploying data and services to multiple datacenters protects your application from major outages in a single datacenter.

Azure Traffic Manager

Once a datacenter-specific failure occurs, you must redirect traffic to services or deployments in another datacenter. This routing can be done manually, but it is more efficient to use an automated process. Azure Traffic Manager (WATM) is designed for this task. It allows you to automatically manage the failover of user traffic to

another datacenter in case the primary datacenter fails. Because traffic management is an important part of the overall strategy, it is important to understand the basics of WATM.
In the diagram below, users connect to a URL specified for WATM (**http://myATMURL.trafficmanager.net**) that abstracts the actual site URLs (**http://app1URL.cloudapp.net** and **http://app2URL.cloudapp.net**). Based on how you configure the criteria for when to route users, they will be sent to the correct actual site when the policy dictates. The policy options are round-robin, performance, or failover. For the sake of this whitepaper we will only be concerned with the option of failover.

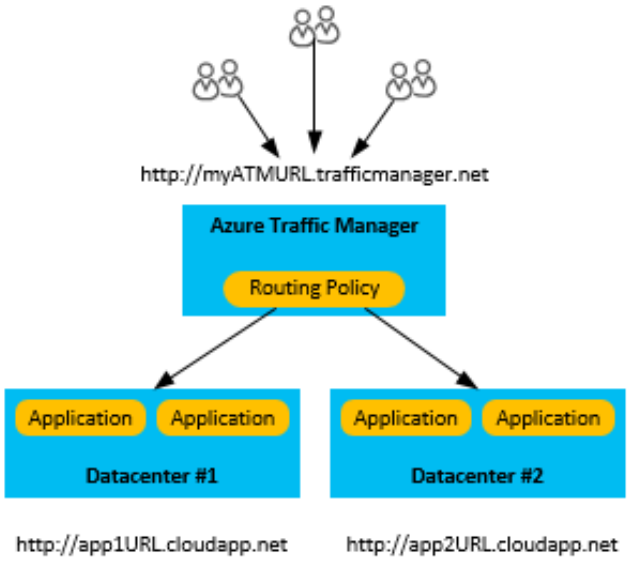


Figure 5 Routing using the Azure Traffic Manager

When configuring WATM you will provide a new Traffic Manager DNS prefix. This is the URL prefix you will provide to your users to access your service. WATM now abstracts load balancing one level up and not at the datacenter level. The Traffic Manager DNS maps to a CNAME for all the deployments it manages.
Within WATM, you specify the priority of the deployments that users will be routed to when failure occurs. The WATM monitors the endpoints of the deployments and notes when the primary deployment fails. At failure, WATM will analyze the prioritized list of deployments and route users to the next one on the list.
While WATM decides where to go in a failover, you can decide if your failover domain is dormant or active while NOT in failover mode. That functionality has nothing to do with Azure Traffic Manager. WATM detects a failure in the primary site and goes to rollover to the failover site. WATM rolls over regardless of whether that site is currently actively serving users or not. More information about dormant or active failover domains can be found in later sections of this paper.
For more information on how Azure Traffic Manager works please refer to the following links.

- Traffic Manager Overview
- Traffic Manager Configuration Tasks

Common Azure Disaster Scenarios

The following sections cover several different types of disaster scenarios. Datacenter failure is not the only cause of application-wide failures. Poor design or administration errors can also lead to outages. It is important to consider the possible causes of a failure during both the design and testing phases of your recovery plan. A good plan takes advantage of Azure features and augments them with application-specific strategies. The chosen response is dictated by the importance of the application, the RPO, and the RTO.

Application Failure

As mentioned previously, Azure Fabric Controller automatically handles failures resulting from the underlying hardware or operating system software in the host virtual machine. Azure creates a new instance of the role on a functioning server and adds it to the load balancer rotation. If the number of role instances is greater than one, Azure shifts processing to the other running role instances while replacing the failed node.

There are serious application errors that happen independently of any hardware or operating system failures. The application could fail due to the catastrophic exceptions caused by bad logic or data integrity issues. You must incorporate enough telemetry into the code so that a monitoring system can detect failure conditions and notify an application administrator. The administrator with full knowledge of the disaster recovery processes can make a decision to invoke a failover process. Alternatively, the administrator could simply accept an availability outage to resolve the critical errors.

Data Corruption

Azure automatically stores your Azure SQL Database and Azure Storage data three times redundantly within different fault domains in the same datacenter. If geo-replication is used, it is stored three additional times in a different datacenter. However, if your users or your application corrupts that data in the primary copy, it quickly replicates to the other copies. Unfortunately, this results in three copies of corrupt data.

To manage potential corruption of your data, you have two options. First, you can manage a custom backup strategy. You can store your backups in Azure or on-premises depending on your business requirements or governance regulations. Another option is to use the new Point in Time Restore database recovery option for SQL database. For more information, see the section on Data Strategies for Disaster Recovery.

Network Outage

When parts of the Azure network are down, you may not be able to get to your application or data. If one or more role instances are unavailable due to network issues, Azure leverages the remaining available instances of your application. If your application can't access its data because of an Azure network outage, you can potentially run in a degraded mode locally by using cached data. You need to architect the disaster recovery strategy for running in degraded mode in your application. For some applications, this might not be practical. Another option is to store data in an alternate location until connectivity is restored. If degraded mode is not an option, the remaining options are application downtime or failover to an alternate datacenter. The design of an application running in degraded mode is a much a business decision as a technical one. This is discussed further in the section on Degraded Application Functionality.

Failure of Dependent Service

Azure provides many services that can experience periodic downtime. Consider Azure Shared Caching as an example. This multitenant service provides caching capabilities to your application. It is important to consider what happens in your application if the dependent service is unavailable. In many ways, this scenario is similar to the network outage scenario. However, considering each service independently results in potential improvements to your overall plan.

For example, with caching, there is a relatively new alternative to the multitenant Shared Caching model. Azure Caching on roles provides caching to your application from within your cloud service deployment. (This is also the recommended way to use Caching going forward). While it has a limitation of only being accessible from within a single deployment, there are potential disaster recovery benefits. First, the service now runs on roles that are local to your deployment. Therefore, you are better able to monitor and manage the status of the cache as part of your overall management processes for the cloud service. However, this type of caching also exposes new features. One of the new features is high availability for cached data. This helps to preserve cached data in the event that a single node fails by maintaining duplicate copies on other nodes. Note that high availability decreases throughput and increases latency because of the updating of the secondary copy on writes. It also doubles the amount of memory used for each item, so plan for that. This specific example demonstrates that each dependent service might have capabilities that improve your overall availability and resistance to catastrophic failures.

With each dependent service, you should understand the implications of a total outage. In the Caching example, it might be possible to access the data directly from a database until you restore the Caching capabilities. This would be a degraded mode in terms of performance but would provide full functionality with regard to data.

Datacenter Down

The previous failures have primarily been failures that can be managed within the same Azure datacenter. However, you must also prepare for the possibility that there is an outage of the entire datacenter. When a datacenter goes down, the locally redundant copies of your data are not available. If you have enabled Geo-replication, there are three additional copies of your blobs and tables in a datacenter in a different region. When Microsoft declares the datacenter lost, Azure remaps all of the DNS entries to the geo-replicated datacenter. Note that you do not have any control over this process, and it will only occur for datacenter-wide failures. Because of this, you must also rely on other application-specific backup strategies to achieve the highest level of availability. For more information, see the section on Data Strategies for Disaster Recovery.

Azure Down

In disaster planning, you must consider the entire range of possible disasters. One of the most severe outages would involve all Azure datacenters simultaneously. As with other outages, you might decide that you will take the risk of temporary downtime in that event. Widespread failures that span datacenters should be much rarer than isolated failures involving dependent services or single datacenters. However, for some mission critical applications, you might decide that there must be a backup plan for this scenario as well. The plan for this event could include failing over to services in an Alternative Clouds or a Hybrid On-Premises and Cloud Solutions.

Degraded Application Functionality

A well designed application typically uses a collection of modules that communicate with each other though the implementation of loosely coupled information interchange patterns. A DR-friendly application particularly requires separation of tasks at the module level. This is to prevent an outage of a dependent service from bringing down the entire application. For example, consider a web commerce application for Company Y; the following modules might constitute the application:

- **Product Catalog:** allows the users to browse products
- **Shopping Cart:** allows users to add/remove products in their shopping cart
- **Order Status:** shows the shipping status of user orders
- **Order Submission:** finalizes the shopping session by submitting the order with payment
- **Order Processing:** validates the order for data integrity and performs quantity availability check

When a dependent of a module in this application goes down, how does the module function until that part recovers? A well architected system implements isolation boundaries through separation of tasks both at design time and run time. You can categorize every failure as recoverable and non-recoverable. Non-recoverable errors will take down the module, but you can mitigate a recoverable error through alternatives. As discussed in the high availability section, you can hide some problems from users by handling faults and taking alternate actions. During a more serious outage, the application might be completely unavailable. However, a third option is to continue servicing users in degraded mode.
For instance, if the database for hosting orders goes down, the Order Processing module loses its ability to process sales transactions. Depending on the architecture, it might be hard or impossible for the Order Submission and Order Processing parts of the application to continue. If the application is not designed to handle this scenario, the entire application might go offline.
However, in this same scenario, it is possible that the product data is stored in a different location. In that case, the Product Catalog module can still be used for viewing products. In degraded mode, the application continues to be

available to users for available functionality like viewing the product catalog. Other parts of the application, however, are unavailable, such as ordering or inventory queries.
Another variation of degraded mode centers on performance rather than capabilities. For example, consider a scenario where the product catalog was being cached with Azure Caching. If Caching became unavailable, it is possible that the application could go directly to the server storage to retrieve product catalog information. But this access might be slower than the cached version. Because of this, the application performance is degraded until the Caching service is fully restored.
Deciding how much of an application will continue to function in degraded mode is both a business and a technical decision. The application must also decide how to inform the users of the temporary problems. In this example, the application could allow viewing products and even adding them to a shopping cart. However, when the user attempts to make a purchase, the application notifies the user that the sales module is down temporarily. It is not ideal for the customer, but it does prevent an application-wide outage.

Data Strategies for Disaster Recovery

Handling data correctly is the hardest area to get right in any disaster recovery plan. Restoring data is also the part of the recovery process that typically takes the most time. Different choices in degradation modes result in difficult challenges for data recovery from failure and consistency after failure. One of the factors is the need to restore or maintain a copy of the application's data. You will use this data for referential and transactional purposes at a secondary site. An on-premises setting requires an expensive and lengthy planning process to implement a multi-datacenter DR strategy. Conveniently, most cloud providers, including Azure, readily allow the deployment of applications to multiple datacenters. These datacenters are geographically located in such a way that multi-datacenter outages should be extremely rare. The strategy for handling data across datacenters is one of the contributing factors for the success of any disaster recovery plan.
The following sections discuss disaster recovery techniques related to data backups, reference data, and transactional data.

Backup and Restore

Regular backups of application data can support some disaster recovery scenarios. Different storage resources require different techniques.
For the Basic, Standard, and Premium SQL Database tiers, you can take advantage of Point in Time Restore to recover your database. For more information, see Point in Time Restore for Azure SQL Database. Another option is to use Active Geo-Replication for SQL Database. This automatically replicates database changes to secondary databases in the same Azure region or even in a different Azure region. This provides a potential alternative to some of the more manual data synchronization techniques presented in this paper. For more information, see Active Geo-Replication for Azure SQL Database.
You can also use a more manual approach for backup and restore. Use the DATABASE COPY command to create a copy of the database. You must use this command to get a backup with transactional consistency. You can also leverage the import/export service of Azure SQL Database. This supports exporting databases to BACPAC files that are stored in Azure Blob storage. The built-in redundancy of Azure Storage creates two replicas of the backup file in the same datacenter. However, the frequency of running the backup process determines your RPO, which is the amount of data you might lose in disaster scenarios. For example, you perform a backup at the top of the hour, and disaster occurs two minutes before the top of the hour. You lose 58 minutes of data that happened after the last backup was performed. Also, to protect against a datacenter outage, you should copy the BACPAC files to an alternate datacenter. You then have the option of restoring those backups in the alternate datacenter. For more details, see Business Continuity in Azure SQL Database.
For Azure Storage, you can develop your own custom backup process or use one of many third-party backup tools. Note that there are additional complexities in most application designs where storage resources reference each other. For example, consider a SQL Database that has a column that links to a blob in Azure Storage. If the backups do not happen simultaneously, the database might have the pointer to a blob that was not backed-up before the failure. The application or disaster recovery plan must implement processes to handle this inconsistency after a recovery.

Reference Data Pattern (Disaster Recovery)

As mentioned previously, reference data is read-only data that supports application functionality. It typically does not change frequently. Although backup and restore is one method to handle datacenter outages, the RTO is relatively long. When you deploy the application to a secondary datacenter, there are some strategies that improve the RTO for reference data.

Because reference data changes infrequently, you can improve the RTO by maintaining a permanent copy of the reference data in the secondary datacenter. This eliminates the time required to restore backups in the event of a disaster. To meet the multi-datacenter DR requirements, you must deploy the application and the reference data together on multiple datacenters. As mentioned in Reference Data Pattern (High Availability), you can deploy reference data to the role itself, external storage, or a combination of both. The intra compute node reference data deployment model implicitly satisfies the DR requirements. Reference data deployment to SQL Database requires that you deploy a copy of the reference data to each datacenter. The same strategy applies to Azure Storage. You must deploy a copy of any reference data stored on Azure Storage to the primary and the secondary datacenters.

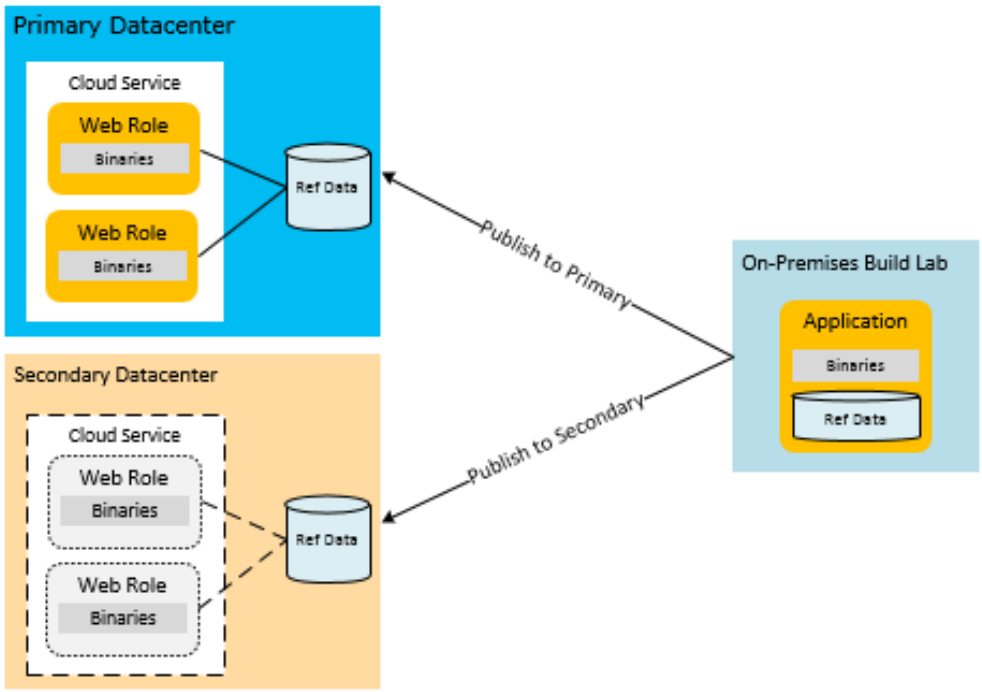


Figure 6 Reference data publication to both primary and secondary datacenters

As mentioned previously, you must implement your own application-specific backup routines for all data, including reference data. Geo-replicated copies across datacenters are only used in a datacenter-wide outage. To prevent extended downtime, deploy the mission critical parts of the application's data to the secondary datacenter. For an example of this topology, see the Active/Passive model.

Transactional Data Pattern (Disaster Recovery)

Implementation of a fully functional disaster mode strategy requires asynchronous replication of the transactional data to the secondary datacenter. The practical time windows within which the replication can occur will determine the RPO characteristics of the application. You might still recover the data lost from the primary datacenter during the replication window. You may also be able to merge with the secondary datacenter later.

The following architecture examples provide some ideas on different ways of handling transactional data in a failover scenario. It is important to note that these examples are not exhaustive. For example, intermediate storage locations such as queues could be replaced with Azure SQL Database. The queues themselves could be either Azure Storage or Service Bus queues (see Azure Queues and Azure Service Bus Queues - Compared and Contrasted). Server storage destinations could also vary, such as Azure tables instead of SQL Database. In addition, there might be worker roles that are inserted as intermediaries in various steps. The important thing is not to

emulate these architectures exactly, but to consider various alternatives in the recovery of transactional data and related modules.
Consider an application that uses Azure Storage queues to hold transactional data. This allows worker roles to process the transactional data to the server database in a decoupled architecture. As discussed, this requires the transactions to use some form of temporary caching if the front-end roles require the immediate query of that data. Depending on the level of data loss tolerance, you could choose to replicate the queues, the database, or all of the storage resources. With only database replication, if the primary datacenter goes down, you can still recover the data in the queues when the primary datacenter comes back. The following diagram shows an architecture where the server database is synchronized across datacenters.

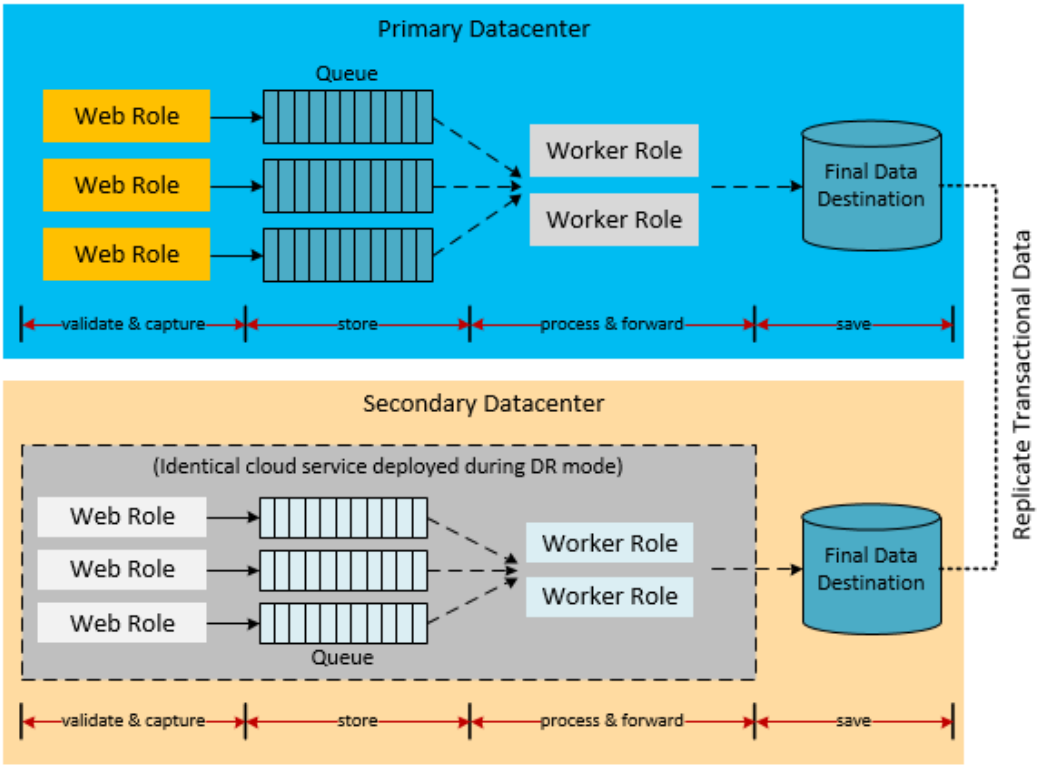


Figure 7 Replicate transactional data in preparation for DR

The biggest challenge to implement the previous architecture is the replication strategy between datacenters. Azure provides a SQL Data Sync service for this type of replication. However, the service is still in preview and is not recommended for production environments. For more information, see Business Continuity in Azure SQL Database. For production applications, you must invest in a third-party solution or create your own replication logic in code. Depending on the architecture, the replication might be bi-directional, which is also more complex. One potential implementation could make use of the intermediate queue in the previous example. The worker role that processes the data to the final storage destination could make the change in both the primary and secondary datacenters. These are not trivial tasks, and complete guidance for replication code is beyond the scope of this paper. The important point is that a lot of your time and testing should focus on how you replicate your data to the secondary datacenter. Additional processing and testing should be done to ensure that the failover and recovery processes correctly handle any possible data inconsistencies or duplicate transactions.

Note

Most of this paper focuses on Platform as a Service. However, there are additional replication and availability options for hybrid applications that use Azure Virtual Machines. These hybrid applications use Infrastructure as a Service (IaaS) to host SQL Server on virtual machines in Azure. This allows traditional availability approaches in SQL Server, such as AlwaysOn Availability Groups

or Log Shipping. Some techniques, such as AlwaysOn, only work between on-premises SQL Servers and Azure virtual machines. For more information, see High Availability and Disaster Recovery for SQL Server in Azure Virtual Machines.

Consider a second architecture that operates in degraded mode. The application on the secondary datacenter deactivates all the functionality, such as reporting, BI, or draining queues. It only accepts the most important types of transactional workflows as defined by business requirements. The system captures the transactions and writes them to queues. The system may postpone processing the data during the initial stage of the outage. If the system on the primary datacenter reactivates within the expected time window, the worker roles in the primary datacenter can drain the queues. This process eliminates the need for database merging. If the primary datacenter outage goes beyond the tolerable window, the application can start processing the queues. In this scenario, the database on the secondary contains incremental transactional data that must be merged once the primary reactivates. The following diagram shows this strategy for temporarily storing transactional data until the primary datacenter is restored.

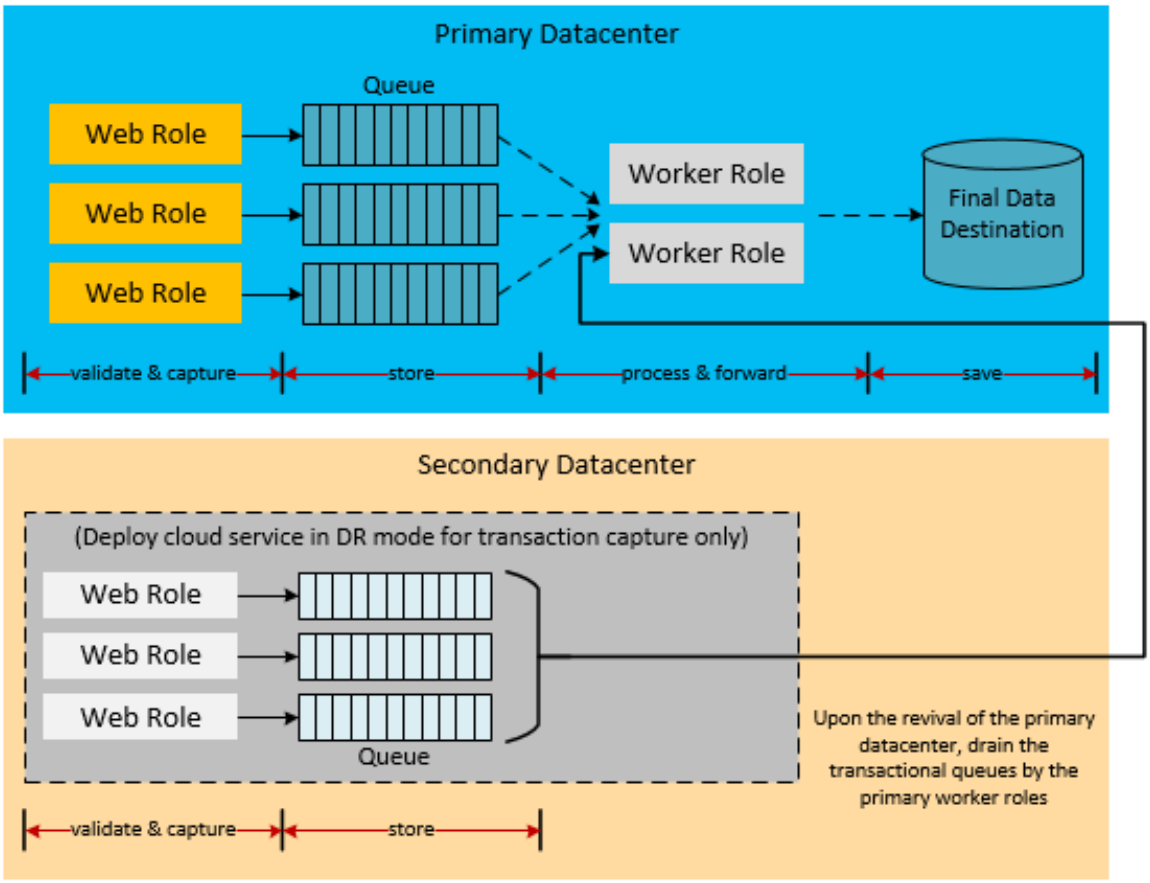


Figure 8 Degraded application mode for transaction capture only

For more discussion of data management techniques for resilient Azure applications, see Failsafe: Guidance for Resilient Cloud Architectures.

Deployment Topologies for Disaster Recovery

Prepare mission critical applications for the eventuality of the entire datacenter going down. You do this by incorporating a multi-datacenter deployment strategy into the operational planning. Multi-datacenter deployments might involve IT Pro processes to publish the application and reference data to the secondary datacenter after experiencing a disaster. If the application requires instant failover, the deployment process may involve an active/passive or an active/active setup. This type of deployment has existing instances of the

application running in the alternate datacenter. As discussed, a routing tool such as the Azure Traffic Manager provides load balancing services at the DNS level. It can detect outages and route the users to different datacenters when needed.
Part of a successful Azure disaster recovery is architecting that recovery into the solution from the start. The cloud provides additional options for recovering from failures during a disaster that are not available in a traditional hosting provider. Specifically, you can dynamically and quickly allocate resources to a different datacenter. Therefore, you won't pay a lot for idle resources while waiting for a failure to occur.
The following sections cover different deployment topologies for disaster recovery. Typically, there is a tradeoff in increased cost or complexity for additional availability.

Single-Region Deployment

A single-region deployment is not really a disaster recovery topology, but is meant to contrast the other architectures. Single-region deployments are common for applications in Azure. It is not, however, a serious contender for a disaster recovery plan. The following diagram depicts an application running in a single Azure datacenter. As discussed previously, the Azure Fabric Controller and the use of fault and upgrade domains increase availability of the application within the datacenter.

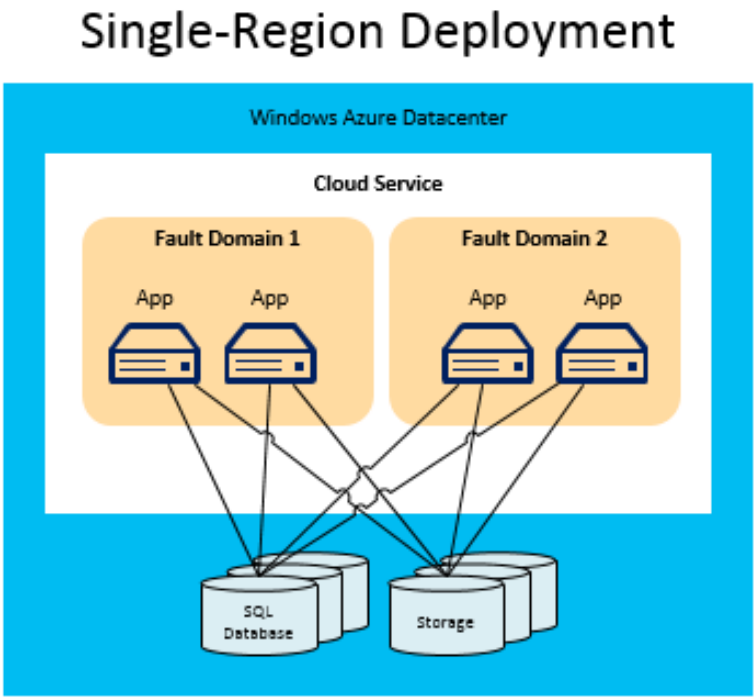


Figure 9 Single Region Deployment

Here it is apparent that the database is a single point of failure. Even though Azure replicates the data across different fault domains to internal replicas, this all occurs in the same datacenter. It cannot withstand a catastrophic failure. If the datacenter goes down, all of the fault domains go down, which includes all service instances and storage resources.
For all but the least critical applications, you must devise a plan to deploy your application across multiple datacenters in different regions. You should also consider RTO and cost constraints in considering which deployment topology to use.
Let's take a look now at specific patterns to support failover across different datacenters. These examples all use two datacenters to describe the process.

Redeploy

In this pattern, only the primary datacenter has applications and databases running. The secondary datacenter is not set up for an automatic failover. So when disaster occurs, you must spin up all the parts of the service in the

new datacenter. This includes uploading a cloud service to Azure, deploying the cloud services, restoring the data, and changing the DNS to reroute the traffic.
While this is the most affordable of the multi-region options, it has the worst RTO characteristics. In this model, the service package and database backups are stored either on-premises or in the blob storage of the secondary datacenter. However, you must deploy a new service and restore the data before it resumes operation. Even if you fully automate the data transfer from backup storage, spinning up the new database environment consumes a lot of time. Moving data from the backup disk storage to the empty database on the secondary datacenter is the most expensive part of restore. You must do this, however, to bring the new database to an operational state since it is not replicated.
The best approach is to store the service packages in Azure Blob storage in the secondary datacenter. This eliminates the need to upload the package to Azure, which is what happens when you deploy from an on-premises development machine. You can quickly deploy the service packages to a new cloud service from blob storage by using PowerShell scripts.
This option is only practical for non-critical applications that can tolerate a high RTO. For instance, this might work for an application that can be down for several hours, but should be running again within 24 hours.

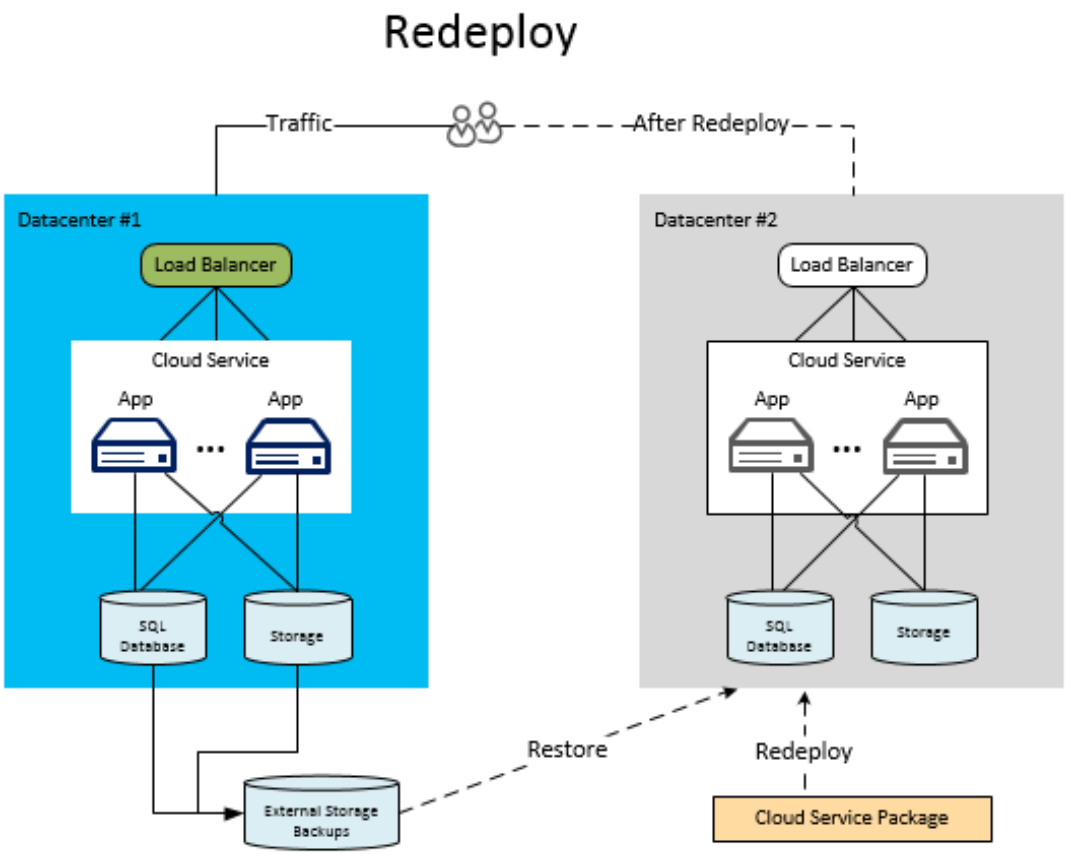


Figure 10 Redeploy to a secondary Azure datacenter

Active/Passive

The Active/Passive pattern is the choice that many companies favor. This pattern provides improvements to the RTO with a relatively small increase in cost over the redeploy pattern. In this scenario, there is again a primary and a secondary Azure datacenter. All of the traffic goes to the active deployment on the primary datacenter. The secondary datacenter is better prepared for disaster recovery because the database is running on both datacenters. Additionally, there is a synchronization mechanism in place between them. This standby approach can involve two variations: a database-only approach or a complete deployment in the secondary datacenter.
In the first variation of the Active/Passive pattern, only the primary datacenter has a deployed cloud service application. However, unlike the redeploy pattern, both datacenters are synchronized with the contents of the database (see the section on[Transactional Data Pattern (Disaster Recovery)](#)). When a disaster occurs, there are

fewer activation requirements. You start the application in the secondary datacenter, change connection strings to the new database, and change the DNS entries to reroute traffic.
Like the redeploy pattern, you should already have stored the service packages in Azure Blob storage in the secondary datacenter for faster deployment. Unlike the redeployment pattern, you don't incur the majority of the overhead that database restore operations requires. The database is ready and running. This saves a significant amount of time, making this an affordable and, therefore, the most popular DR pattern.

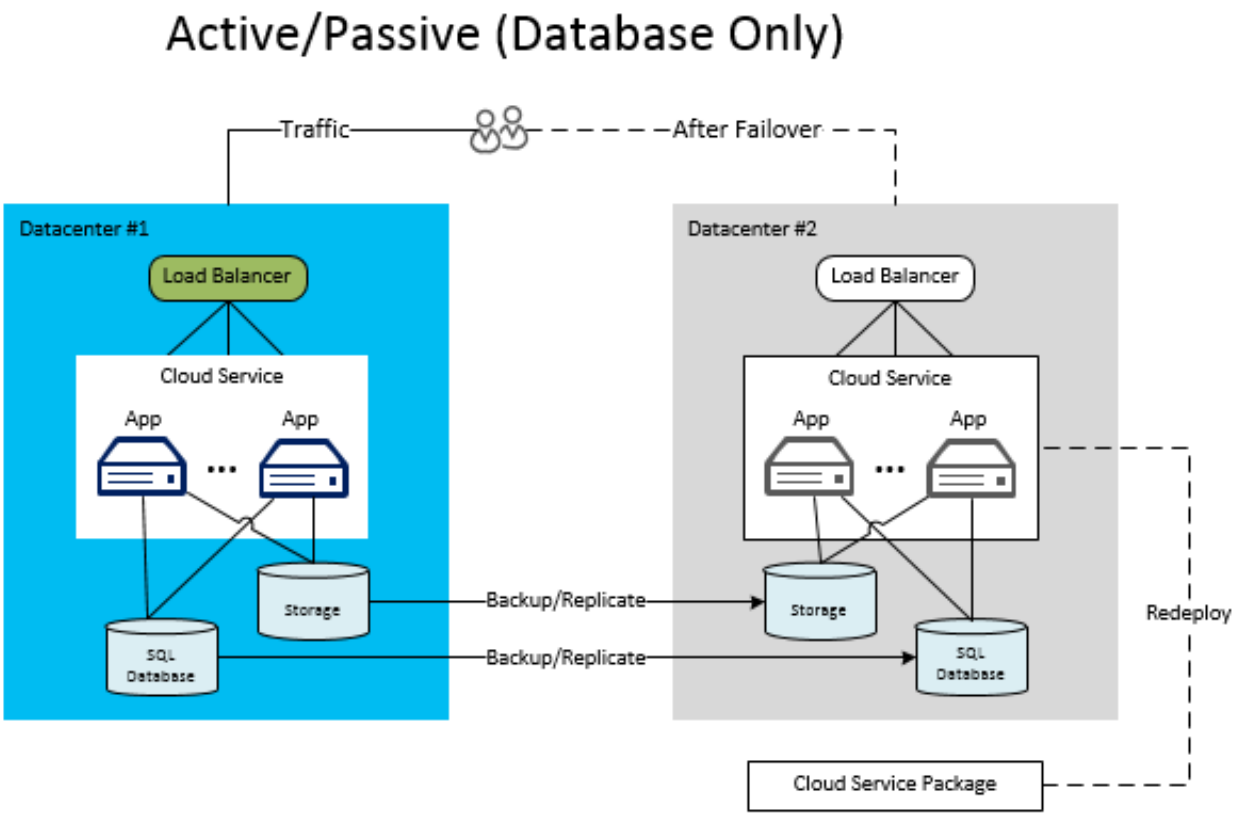


Figure 11 Active/Passive (Database Only)
In the second variation of the Active/Passive pattern, the primary and secondary datacenters have a full deployment. This deployment includes the cloud services and a synchronized database. However, only the primary datacenter is actively handling network requests from the users. The secondary datacenter becomes active only when the primary datacenter goes down. In that case, all new network requests route to the secondary region. Azure Traffic Manager can manage this failover automatically.
Failover occurs faster than the database-only variation because the services are already deployed. This pattern provides a very low RTO; the secondary failover datacenter must be ready to go immediately after failure of the primary datacenter.
Along with quicker response, this pattern also has an additional advantage of pre-allocating and deploying backup services. You don't have to worry about a datacenter not having the space to allocate new instances in a disaster. This is important if your secondary Azure datacenter is nearing capacity. There is no guarantee (SLA) that you will instantly be able to deploy a number of new cloud services in any datacenter.
For the fastest response time with this model, you must have similar scale (number of role instances) in the primary and secondary datacenters. Despite the advantages, paying for unused compute instances is costly, and this is often not the most prudent financial choice. Because of this, it is more common to use a slightly scaled-down version of cloud services on the secondary datacenter. Then you can quickly failover and scale out the secondary deployment when necessary. You should automate the failover process so that, once the primary datacenter fails, you activate additional instances depending up on the load. This could involve some type of automatic scaling mechanism, such as the AutoScale Preview or the The Autoscaling Application Block. The following diagram shows the model where the primary and secondary datacenters contain a fully deployed cloud service in an Active/Passive pattern.

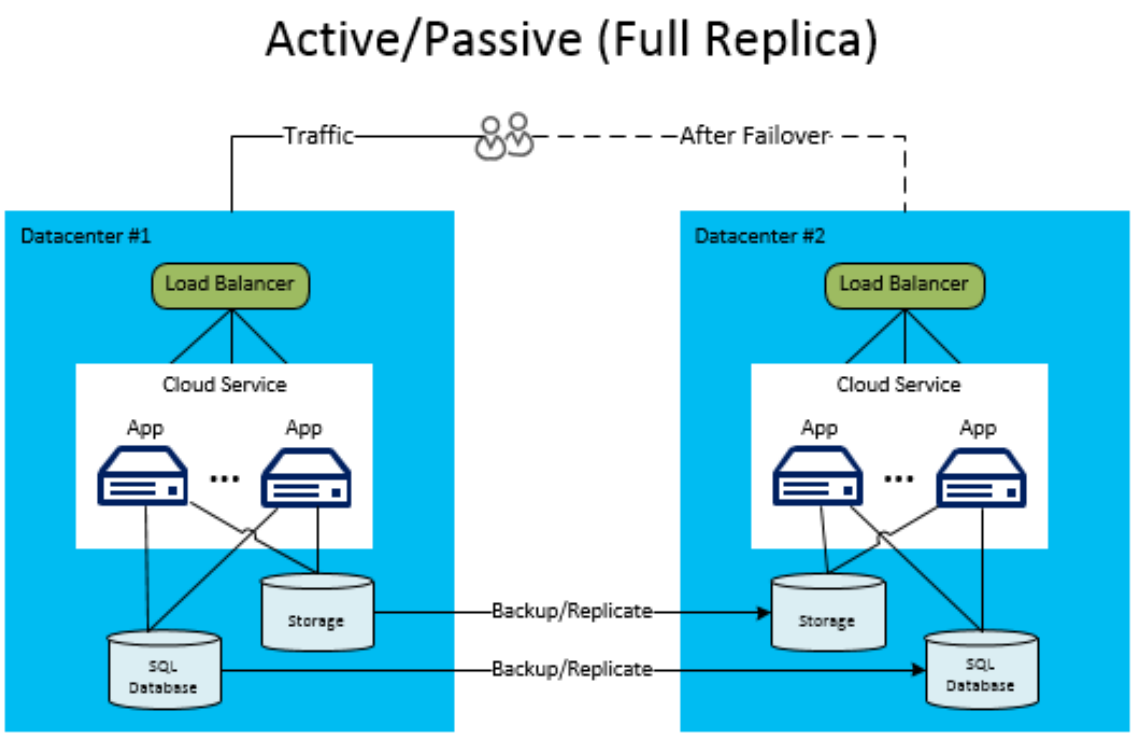


Figure 12 Active/Passive (Full Replica)

Active/Active

By now, you're probably figuring out the evolution of the patterns – decreasing the RTO increases costs and complexity. The Active/Active solution actually breaks this tendency with regard to cost. In an Active/Active pattern, the cloud services and database are fully deployed in both datacenters. Unlike the Active/Passive model, both datacenters receive user traffic. This option yields the quickest recovery time. The services are already scaled to handle a portion of the load at each datacenter. The DNS is already enabled to use the secondary datacenter. There is additional complexity in determining how to route users to the appropriate datacenter. Round-robin scheduling might be possible. It is more likely that certain users would use a specific datacenter where the primary copy of their data resides.

In case of failover, simply disable DNS to the primary datacenter, which routes all traffic to the secondary datacenter. Even in this model, there are some variations. For example, the following diagram shows a model where the primary datacenter owns the master copy of the database. The cloud services in both datacenters write to that primary database. The secondary deployment can read from the primary or replicated database. Replication in this example happens one way.

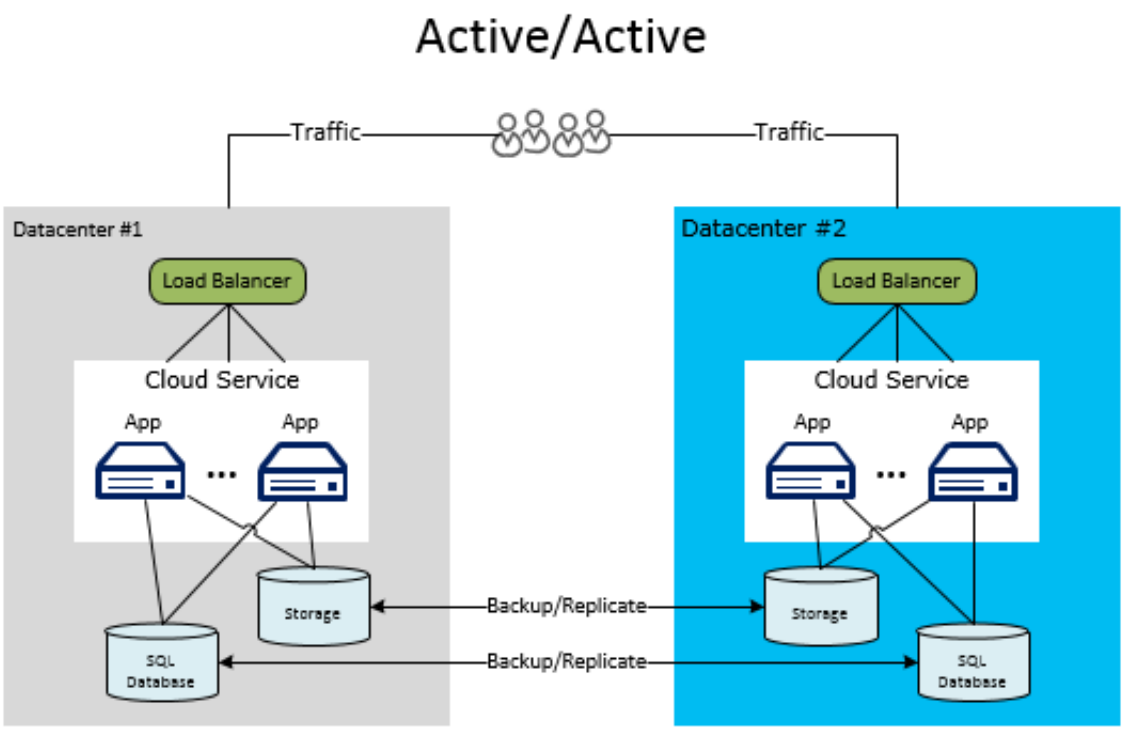


Figure 13 Active/Active

There is a downside to the Active/Active architecture in the previous diagram. The second datacenter must access the database in the first datacenter because the master copy resides there. Performance significantly drops off when you access data from outside a datacenter. In cross-datacenter database calls, you should consider some type of batching strategy to improve the performance of these calls. For more information, see Batching Techniques for SQL Database Applications in Azure. An alternative architecture could involve each datacenter accessing its own database directly. In that model, some type of bidirectional replication would be required to synchronize the databases in each datacenter.

In the Active/Active pattern, you might not need as many instances on the primary datacenter as you would in the Active/Passive pattern. If you have ten instances on the primary datacenter in an Active/Passive architecture, you might need only five in each datacenter in an Active/Active architecture. Both regions now share the load. This could be a cost savings over the Active/Passive pattern if you kept a warm standby on the passive datacenter with ten instances waiting for failover.

Realize that until you restore the primary datacenter, the secondary datacenter may receive a sudden surge of new users. If there were 10,000 users on each server when the primary datacenter fails, the secondary datacenter suddenly has to handle 20,000 users. Monitoring rules on the secondary datacenter must detect this increase and double the instances in the secondary datacenter. For more information on this, see the section on Failure Detection.

Hybrid On-Premises and Cloud Solutions

One additional strategy for disaster recovery is to architect a hybrid application that runs on-premises and in the cloud. Depending on the application, the primary datacenter might be either location. Consider the previous architectures and imagine the primary or secondary datacenters as an on-premises location.

There are some challenges in these hybrid architectures. First, most of this paper has addressed Platform as a Service (PaaS) architecture patterns. Typical PaaS applications in Azure rely on Azure-specific constructs such as roles, cloud services, and the Fabric Controller. To create an on-premises solution for this type of PaaS application would require a significantly different architecture. This might not be feasible from a management or cost perspective.

However, a hybrid solution for disaster recovery has fewer challenges for traditional architectures that have simply moved to the cloud. This is true of architectures that use Infrastructure as a Service (IaaS). IaaS applications use Virtual Machines in the cloud that can have direct on-premises equivalents. The use of virtual networks also allows

you to connect machines in the cloud with on-premises network resources. This opens up several possibilities that are not possible with PaaS-only applications. For example, SQL Server can take advantage of disaster recovery solutions such as AlwaysOn Availability Groups and database mirroring. For details, see High Availability and Disaster Recovery for SQL Server in Azure Virtual Machines.

IaaS solutions also provide an easier path for on-premises applications to use Azure as the failover option. You might have a fully functioning application in an existing on-premises datacenter. However, what if you lack the resources to maintain a geographically separate datacenter for failover? You might decide to use Virtual Machines and Virtual Networks to get your application running in Azure. Define processes that synchronize data to the cloud. The Azure deployment then becomes the secondary datacenter to use for failover. The primary datacenter remains the on-premises application. For more information about IaaS architectures and capabilities, see Virtual Machines and Virtual Network.

Alternative Clouds

There are situations when even the robustness of Microsoft's cloud might not be enough for your availability requirements. In the past year or so, there have been a few severe outages of various cloud platforms. This includes Amazon Web Services (AWS) and the Azure platforms. Even the best preparation and design to implement backup systems during a disaster fall short and your entire cloud takes the day off.

You'll want to compare availability requirements with the cost and complexity of increased availability. Perform a risk analysis, and define the RTO and RPO for your solution. If your application cannot tolerate any downtime, it might make sense for you to consider using another cloud solution. Unless the entire Internet goes down simultaneously, another cloud solution, such as Rackspace or Amazon Web Services, will be still functioning on the rare chance that Azure is completely down.

As with the hybrid scenario, the failover deployments in the previous DR architectures can also exist within another cloud solution. Alternative cloud DR sites should only be used for those solutions with an RTO that allows very little, if any, downtime. Note that a solution that uses a DR site outside of Azure will require more work to configure, develop, deploy, and maintain. It is also more difficult to implement best practices in a cross-cloud architecture. Although cloud platforms have similar high-level concepts, the APIs and architectures are different. Should you decide to split your DR among different platforms, it would make sense to architect abstraction layers in the design of the solution. If you do this, you won't need to develop and maintain two different versions of the same application for different cloud platforms in case of disaster. As with the hybrid scenario, the use of Virtual Machines might be easier in these cases than cloud-specific PaaS designs.

Automation

Some of the patterns we just discussed require quick activation of off-line deployments as well as restoration of specific parts of a system. Automation, or scripting, supports the ability to activate resources on-demand and deploy solutions rapidly. In this paper, DR-related automation is equated with Azure PowerShell, but the Service Management REST API is also an option. Developing scripts helps to manage the parts of DR that Azure does not transparently handle. This has the benefit of producing consistent results each time, which minimizes the chance of human error. Having pre-defined DR scripts also reduces the time to rebuild a system and its constituent parts in the midst of a disaster. You don't want to try to manually figure out how to restore your site while it is down and losing money every minute.

Once you create the scripts, test them over and over from start to finish. After you verify their basic functionality, make sure that you test them in Disaster Simulation. This helps uncover flaws in the scripts or processes.

A best practice with automation is to create a repository of Azure DR PowerShell scripts. Cleary mark and categorize them for easy lookup. Designate one person to manage the repository and versioning of the scripts. Document them well with explanations of parameters and examples of script use. Also ensure that you keep this documentation in sync with your Azure deployments. This underscores the purpose of having one person in charge of all parts of the repository.

Failure Detection

In order to correctly handle problems with availability and disaster recovery, you must be able to detect and diagnose failures. You should do advanced server and deployment monitoring so you can quickly know when a

system or its parts are suddenly down. Monitoring tools that look at the overall health of the cloud Service and its dependencies can perform part of this work. One Microsoft tool is System Center 2012 R2 (SCOM). Other third-party tools, such as AzureWatch, can also provide monitoring capabilities. AzureWatch also allows you to automate scalability. Most monitoring solutions track key performance counters and service availability.
Although these tools are vital, they do not replace the need to plan for fault detection and reporting within a cloud service. You must plan to properly use Azure diagnostics. Custom performance counters or event log entries can also be part of the overall strategy. This provides more data during failures to quickly diagnose the problem and restore full capabilities. It also provides additional metrics for the monitoring tools to use to determine application health. For more information, see Collect Logging Data by Using Azure Diagnostics. For a discussion of how to plan for an overall "health model", see Failsafe: Guidance for Resilient Cloud Architectures.

Disaster Simulation

Simulation testing involves creating small real life situations on the actual work floor to observe how the team members react. Simulations also show how effective the solutions are outlined in the recovery plan. Carry out simulations in such a way that the scenarios created do not disrupt actual business while still feeling like "real" situations.
Consider architecting a type of "switchboard" in the application to manually simulate availability issues. For instance, through a soft switch, trigger database access exceptions for an ordering module by causing it to malfunction. Similar lightweight approaches can be taken for other modules at the network interface level.
Any issues that were inadequately addressed are highlighted during simulation. The simulated scenarios must be completely controllable. This means that, even if the recovery plan seems to be failing, you can restore the situation back to normal without causing any significant damage. It's also important that you inform higher-level management about when and how the simulation exercises will be executed. This plan should include information on the time or resources that may become unproductive while the simulation test is running. When subjecting your disaster recovery plan to a test, it is also important to define how success will be measured.
There are several other techniques that you can use to test disaster recovery plans. However, most of them are simply altered versions of these basic techniques. The main motive behind this testing is to evaluate how feasible and how workable the recovery plan is. Disaster recovery testing focuses on the details to discover holes in the basic recovery plan.

Checklist

Let's summarize the key points that have been covered in this paper. This summary will act as a checklist of items you should consider for your own availability and disaster recovery planning. These are best practices that have been useful for customers seeking to get serious about implementing a successful solution. This type of solution truly works, recovering in a timely and successful manner when system failure hits.

1. Conduct a risk assessment for each application because each can have different requirements. Some applications are more critical than others and would justify the extra cost to architect them for disaster recovery.

2. Use this information to define the RTO and RPO for each application.

3. Design for failure, starting with the application architecture.

4. Implement best practices for high availability, while balancing cost, complexity, and risk.

5. Implement disaster recovery plans and processes.

a. Consider failures that span the module level all the way to a complete cloud outage.

b. Establish backup strategies for all reference and transactional data.

c. Choose a multi-site disaster recovery architecture.

6. Define a specific owner for disaster recovery processes, automation, and testing. The owner should manage and own the entire process.

7. Document the processes so they are easily repeatable. Although there is one owner, multiple people should be able to understand and follow the processes in an emergency.

8. Train the staff to implement the process.

9. Use regular disaster simulations for both training and validation of the process.

Summary

When hardware or software fails within Azure, the techniques and strategies for managing them are different than when failure occurs on on-premise systems. The main reason for this is that cloud solutions typically have more dependencies on infrastructure that's dispersed across the datacenter and managed as separate services. You must deal with partial failures using high availability techniques. To manage more severe failures, possibly due to a disaster event, use disaster recovery strategies.

Azure detects and handles many failures, but there are many types of failures that require application-specific strategies. You must actively prepare for and manage the failures of applications, services, and data.

When creating your application's availability and disaster recovery plan, consider the business consequences of the application's failure. Defining the processes, policies, and procedures to restore critical systems after a catastrophic event takes time, planning, and commitment. And once you establish the plans, you cannot stop there. You must regularly analyze, test, and continually improve the plans based on your application portfolio, business needs, and the technologies available to you. Azure provides both new capabilities and new challenges to creating robust applications that withstand failures.

See Also

Other Resources

Azure Business Continuity Technical Guidance
Business Continuity in Azure SQL Database
High Availability and Disaster Recovery for SQL Server in Azure Virtual Machines
Failsafe: Guidance for Resilient Cloud Architectures
Best Practices for the Design of Large-Scale Services on Azure Cloud Services

ECHO Manufacturer Limited Warranty

(Hardware Repair Service)

The following document details the COBAN Manufacturer Limited Warranty for the ECHO System. COBAN Technologies, Inc. ("COBAN") warrants the COBAN Manufactured ECHO System ("PRODUCT"), against defects in material and workmanship under normal use and service for a period of one (1) year and, such warranties shall begin when the PRODUCT is delivered to the Original End User ("CLIENT"). This expressed Limited Warranty is extended by COBAN to the CLIENT purchasing the PRODUCT for purposes of governmental use only, and is not assignable or transferable to any other party. This is the complete warranty for the PRODUCT manufactured by COBAN and it does not warrant the installation, maintenance, support or service of the PRODUCT unless a separate written agreement is made between COBAN and CLIENT. Please refer to DVMS Maintenance Support Service Option for technical support and software support details.

WARRANTY COVERAGE

The warranty applies within all fifty (50) states of the United States of America. This Limited Warranty is null and void if the factory applied serial number or tamper evident labels have been damaged, altered or removed from the product. COBAN, at their discretion, will at no charge, repair the PRODUCT (with new or reconditioned parts), or replace it with the same or equivalent PRODUCT (using new or reconditioned products), during the warranty period, provided that the CLIENT notifies COBAN according to the terms of this warranty. The repaired or replaced PRODUCT is warranted for the remaining original applicable warranty period. All returned parts of the PRODUCT shall become the property of COBAN.

Items covered under this warranty:

- ECHO Body Camera Module is covered for twelve (12) months under this warranty
- ECHO AC Wall Charger is covered for twelve (12) months under this warranty
- ECHO USB Cable is covered for twelve (12) months under this warranty
- ECHO Clip is covered for twelve (12) months under this warranty
- ECHO POV Camera is covered for twelve (12) months under this warranty
- ECHO Clip Camera is covered for twelve (12) months under this warranty

GENERAL WARRANTY PROVISIONS

This warranty sets forth the extent of COBAN's responsibilities regarding the PRODUCT. Repair and replacement of the purchase price, at COBAN's option, is an exclusive remedy.

THE WARRANTY IS GIVEN IN LIEU OF ALL OTHER EXPRESS WARRANTIES. COBAN DISCLAIMS ALL OTHER WARRANTIES OR CONDITIONS, EXPRESSED OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL COBAN BE LIABLE FOR DAMAGES IN EXCESS OF THE ORIGINAL PURCHASE PRICE OF THE PRODUCT, FOR ANY LOSS OF USE, LOSS OF TIME, INCONVENIENCES, COMMERCIAL LOSS, LOST PROFITS, OR SAVINGS OR OTHER INCIDENTAL, SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PRODUCT TO THE FULL EXTENT THAT MAY BE DISCLAIMED BY LAW.

FORCE MAJEURE

COBAN shall not be liable for delays or failure to perform with respect to this agreement due to force majeure including (i) causes beyond the party's reasonable control and not avoidable by diligence, (ii) acts of God, epidemics, war, riots, or delays in transportation which are beyond the party's reasonable control and not avoidable by diligence, or (iii) inability for causes beyond its control and not avoidable by diligence to obtain necessary labor, materials, or manufacturing facilities, or delays caused by COBANs due to similar causes. In the event of any such delay (each such event being beyond the party's reasonable control and not avoidable by diligence), the date of performance shall be extended for a period equal to the time lost by reason of the delay.

CLIENT'S RESPONSIBILITIES

The CLIENT is responsible for maintaining its own "Disaster Recovery" policies and procedures for the reconstruction of lost or altered files, backup or saving of data or programs to the extent deemed necessary by the CLIENT and for actually reconstructing any lost or altered files, data or programs. COBAN assumes no responsibility for the protection of The CLIENT data. COBAN is not liable for damage to software or data caused

by service to the computer hardware equipment, except to the extent that such damage is caused directly or indirectly by COBAN. Any service / warranty work required on the workstation, server or other devices provide by the CLIENT in conjunction with the DICVS will be performed by the manufacturer's representative from whom they purchased the devices from.

.

CLIENT'S REPRESENTATIVE

At all times during the term of this warranty, at least one (1) employee of the CLIENT shall be designated to act as a Representative. The Representative shall be responsible to react to all equipment problems, attempt troubleshooting to isolate the malfunction area, notify COBAN of the need for service and cooperate with COBAN to diagnose the problem over the telephone.

All initial RMA Requests MUST be called into COBAN's Tech Support line (281-925-0488 option 2) or entered via COBAN Customer Support Web Portal (http://customer.COBANTECH.com**).**
Proof of a bill of sale or purchase order (which is evidence that the PRODUCT is within the warranty period) must be presented to obtain warranty service if requested.

RMA AND SHIPPING

Once COBAN determines that all or part of the PRODUCT requires return for repair or replacement, a Return Merchandise Authorization Number (RMA NUMBER) will be issued. We recommend the CLIENT insure or get a tracking number for the return package as COBAN is not responsible for lost, stolen or damaged packages. Please prominently display the RMA number on the outside of the shipping box and ship labels of each box.

During the first ninety (90) days of deployment, COBAN will cover the cost of any RMA shipment to and from COBAN's maintenance facility. After the ninety (90) days, the CLIENT will be responsible for shipping charges and to insure the product arrives at COBAN intact. COBAN will pay for return shipping, via Ground shipping services to return the repaired/serviced modules back to the CLIENT. Any expedited shipping requests will be the responsibility of and paid for by the CLIENT. Repair times for defective modules are objectives, not guarantees.

ADVANCE PLACEMENT / CROSS SHIP

If advance replacement / cross ship is required and the CLIENT wishes to receive the most expedient service available, the CLIENT will be required to provide COBAN with a credit card authorization to bill the CLIENT's credit card in the event that the CLIENT fails to return the original parts. The credit card will only be charged for COBAN's list price for the part if the part has not been returned within ten (10) days.

Type of Card: _____
Credit Card Number: _____
Expiration Date: _____

OTHER INFORMATION

Unit Replacement
Once a replacement component has been received, the CLIENT must relinquish the defective unit to COBAN. If the defective unit is not returned within ten (10) days, the CLIENT agrees to pay COBAN the cost for the replacement unit upon receipt of invoice. Failure to honor the invoice within ten (10) days after receipt will cause the cancellation of this Service Description Agreement and may result in other legal actions, including but not limited to suspending shipment of subsequent units and or replacement components.
Parts Ownership
All service parts removed from the CLIENT's Supported System become the property of COBAN. The CLIENT will be obligated to pay at the current retail price(s) for any service parts removed from the CLIENT's Supported System and retained by the CLIENT. COBAN will use new and reconditioned parts made by various manufacturers in performing warranty repairs.

NON-WARRANTY SERVICES

Each warranty request pertaining to any item not covered under the ECHO Manufacturer Limited Warranty shall be invoiced to the CLIENT at the agreed upon time and materials rate. Currently, COBAN charges $ 125.00 per hour on non-warranty phone support and $ 95.00 per hour on non-warranty repair. COBAN Support Engineers are not authorized to service any third party hardware, software or vehicle issues.

COBAN will charge the CLIENT a $ 95.00 service fee for any RMA units/components that are returned to COBAN as “non-warranty” items. Non Warranty items are defined under section titled ITEMS NOT COVERED UNDER THIS WARRANTY. Non-Warranty repair work will be billed separately from this service fee.

COBAN will charge the CLIENT a $ 95.00 service fee for any RMA units/components that are returned to COBAN as “non-operational” that are in fact operational (ie: CPU units that have not been ghosted properly, scratched / hazy touch screen monitors, microphones missing parts such as: battery, internal seals, antennas, obvious misuse or damaged systems).

COBAN will obtain approval/direction for any billable service before repairs are initiated (ie. devices not covered, repairs not covered, etc)

COMPLIANCE

FAILURE TO FOLLOW ANY OF THE ABOVE INSTRUCTIONS MAY RESULT IN DELAYS AND MAY CAUSE THE CLIENT TO INCUR ADDITIONAL CHARGES, OR MAY VOID WARRANTY.

IF DURING THE REPAIR OF THE PRODUCT, THE DATA STORED ON THE HARD DRIVE ARE ALTERED, DELETED, OR IN ANY WAY MODIFIED, COBAN IS NOT RESPONSIBLE WHATSOEVER TO RECOVER OR RESTORE SAID DATA. THE CLIENT’S PRODUCT WILL BE RETURNED TO THE CLIENT IN THE ORIGINAL MANUFACTURED CONFIGURATION (SUBJECT TO AVAILABILITY OF SOFTWARE).

ITEMS NOT COVERED UNDER THIS WARRANTY

This warranty does not cover periodically or consumed parts during the life of the product such as but not limited to batteries, cables and wires; loss or damages resulting from external causes such as damaged resulting from dropping of the PRODUCT, collision with any object, fire, flooding, sand, dirt, windstorm, hail, earthquake or damage from exposure to weather conditions, misuse, abuse, damage resulting from improper use of any electrical source, power surges, damage occurring during transport.

This warranty does not cover ancillary equipment not furnished by COBAN, which may be attached to or used in connection with the PRODUCT, or for operation of the PRODUCT with any ancillary equipment. All such ancillary equipment is expressly excluded from this warranty.

All preventive maintenance recommended by COBAN to maintain the product in operating condition is the responsibility of the CLIENT; loss or damage resulting from failure to provide recommended maintenance is not covered under this contract.

- On-site service
- Triage, helpdesk phone support
- Warranty support or service for third party systems
- Data migration
- Normal and customary wear and tear
- Damage due to connection to improper voltage supply
- PRODUCTS that have had the serial numbers removed or made illegible
- Systems that are non operational due to abuse, neglect or improper usage for anything other than what the system was configured to do (not limited to dirt, debris, water damage or liquid of any type)
- A PRODUCT subjected to unauthorized entry or opening, modifications, disassemblies, or repairs (including, without limitation, the addition to the PRODUCT of non-COBAN supplied equipment) that adversely affect performance of the PRODUCT
- Or defects or damage from improper testing, operation, maintenance, installation alteration, modification, or adjustment
- A PRODUCT affected by virus, security breach, or other network related occurrence including but not limited to: installation of third party software applications, network security settings changes resulting in loss of communication, ability to properly use the system or configurations that deviate from the Original Master Gold Image
- A PRODUCT, which, due to illegal or unauthorized alteration of the software / firmware in the PRODUCT, does not function in accordance with COBAN, published specifications or with the FCC type acceptance labeling in effect for the PRODUCT at the time the PRODUCT was initially distributed from COBAN

- Scratches or other cosmetic damages to the PRODUCT's surfaces that do not affect the operation of the PRODUCT

By installing and using the COBAN HARDWARE and SOFTWARE, the CLIENT agrees to be bound by the terms of this WARRANTY STATEMENT.

EDGE HI-DEF / SD 5.7" Manufacturer Limited Warranty

HARDWARE REPAIR SERVICE

The following document details the COBAN Manufacturer Limited Warranty for the EDGE HI-DEF. COBAN Technologies, Inc. ("COBAN") warrants the COBAN Manufactured EDGE HI-DEF System ("PRODUCT"), against defects in material and workmanship under normal use and service for a period of three (3) years and, such warranties shall begin when the PRODUCT is delivered to the Original End User ("CLIENT"). This expressed Limited Warranty is extended by COBAN to the CLIENT purchasing the PRODUCT for purposes of governmental use only, and is not assignable or transferable to any other party. This is the complete warranty for the PRODUCT manufactured by COBAN and it does not warrant the installation, maintenance, support or service of the PRODUCT unless a separate written agreement is made between COBAN and CLIENT. Please refer to DVMS / Command Center Maintenance Support Service Option for technical support and software support details.

WARRANTY COVERAGE

The warranty applies within all fifty (50) states of the United States of America. This Limited Warranty is null and void if the factory applied serial number or tamper evident labels have been damaged, altered or removed from the product. COBAN, at their discretion, will at no charge, repair the PRODUCT (with new or reconditioned parts), or replace it with the same or equivalent PRODUCT (using new or reconditioned products), during the warranty period, provided that the CLIENT notifies COBAN according to the terms of this warranty. The repaired or replaced PRODUCT is warranted for the remaining original applicable warranty period. All returned parts of the PRODUCT shall become the property of COBAN.

Items covered under this warranty:

- EDGE CPU / Encoder Module is covered for three (3) years under this warranty
- EDGE Display Module is covered for three (3) years under this warranty
- EDGE Power Supply Module is covered for three (3) years under this warranty
- EDGE Removable Hard Disk is covered for three (3) years under this warranty
- EDGE System Cables are covered for three (3) years under this warranty
- EDGE Wireless Microphone ("Mic.") Transmitter is covered for three (3) years under this warranty
- EDGE Wireless Mic. Receiver is covered for three (3) years under this warranty
- EDGE Primary Forward Facing Camera is covered for three (3) years under this warranty

WARRANTY LIMITATION

- EDGE System Wires is covered for twelve (12) months under this warranty
- EDGE Power Supply Battery is covered for twelve (12) months under this warranty
- EDGE Wireless Mic. Transmitter Pouch is covered for twelve (12) months under this warranty
- EDGE Wireless Mic. Transmitter Battery is covered for twelve (12) months under this warranty
- EDGE Wireless Mic. Transmitter Antenna is covered for twelve (12) months under this warranty
- EDGE Wireless Mic. Receiver Antennas is covered for twelve (12) months under this warranty
- EDGE Optional Peripheral Devices are coved for twelve (12) months under this warranty

COBAN 3rd Party Warranty and Support

- Support and service on the Dell Servers and Storage is provided by Dell Computer.
  Dell Tech Support: **800-999-3355 ext 7255010** or via Website http://support.dell.com
- Support and service on the IBM Server, Storage, Tape Library and Tivoli Storage Manager Software is provided by IBM. IBM Support: **800-426-7378** or via Website http://www.ibm.com/support/us/en/

GENERAL WARRANTY PROVISIONS

This warranty sets forth the extent of COBAN'S responsibilities regarding the PRODUCT. Repair and replacement of the purchase price, at COBAN'S option, is an exclusive remedy.

THE WARRANTY IS GIVEN IN LIEU OF ALL OTHER EXPRESS WARRANTIES. COBAN DISCLAIMS ALL OTHER WARRANTIES OR CONDITIONS, EXPRESSED OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL COBAN BE LIABLE FOR DAMAGES IN EXCESS OF THE ORIGINAL PURCHASE PRICE OF THE PRODUCT, FOR ANY LOSS OF USE, LOSS OF TIME, INCONVENIENCES, COMMERCIAL LOSS, LOST PROFITS, OR SAVINGS OR OTHER INCIDENTAL, SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PRODUCT TO THE FULL EXTENT THAT MAY BE DISCLAIMED BY LAW

FORCE MAJEURE
COBAN shall not be liable for delays or failure to perform with respect to this agreement due to Force Majeure including (i) causes beyond the party's reasonable control and not avoidable by diligence, (ii) acts of God, epidemics, war, riots, or delays in transportation which are beyond the party's reasonable control and not avoidable by diligence, or (iii) inability for causes beyond its control and not avoidable by diligence to obtain necessary labor, materials, or manufacturing facilities, or delays caused by COBANs due to similar causes. In the event of any such delay (each such event being beyond the party's reasonable control and not avoidable by diligence), the date of performance shall be extended for a period equal to the time lost by reason of the delay.

CLIENT'S RESPONSIBILITIES
It is the CLIENT's responsibility to backup the contents of all hard drives, including any data that may be stored or software that may have been installed on the hard drive. It is possible that the contents of hard drives will be lost or that the drive may need to be reformatted in the course of service and as such COBAN will not be held liable for any damages to or loss of any program, data or other information stored on any media or any part of any PRODUCT serviced hereunder. It is HIGHLY recommended that the CLIENT create a valid disk "image" after final installation is completed. This image will need to be updated as changes are made to the units and kept safe by the CLIENT for data recovery purposes. COBAN assumes no liability or responsibility in developing a disaster recovery policy for the CLIENT. The CLIENT will perform any and ALL data reconstruction, unless specifically stated in the initial contract between COBAN and the CLIENT.

CLIENT'S REPRESENTATIVE
At all times during the term of this warranty, at least one (1) employee of the CLIENT shall be designated to act as Representative. Representative shall be responsible to react to all equipment problems, attempt troubleshoot to isolate the malfunction area, notify COBAN of the need for service and cooperate with COBAN to diagnose the problem over the telephone.

All initial RMA Requests MUST be called into COBAN's Tech Support line (281-925-0488 option 2) or entered via COBAN Customer Support Web Portal (http://customer.COBANTECH.com**).**
Proof of a bill of sale or purchase order (which is evidence that the PRODUCT is within the warranty period) must be presented to obtain warranty service if requested.

RMA AND SHIPPING
Once COBAN determines that all or part of the PRODUCT requires return for repair or replacement, a Return Merchandise Authorization Number (RMA NUMBER) will be issued. We recommend the CLIENT insure or get a tracking number for the return package as COBAN is not responsible for lost, stolen or damaged packages. Please prominently display the RMA number on the outside of the shipping box and ship labels of each box.

During the first ninety (90) days of deployment, COBAN will cover the cost of any RMA shipment to and from COBAN's maintenance facility. After the ninety (90) days, the CLIENT will be responsible for shipping charges and to insure the product arrives at COBAN intact. COBAN will pay for return shipping, via Ground shipping services to return the repaired/serviced modules back to the CLIENT. Any expedited shipping requests will be the responsibility of and paid for by the CLIENT. Repair times for defective modules are objectives, not guarantees.

ADVANCE PLACEMENT / CROSS SHIP
If advance replacement / cross ship is required and the CLIENT wishes to receive the most expedient service available, the CLIENT will be required to provide COBAN with a credit card authorization to bill the CLIENT's credit card in the event that the CLIENT fails to return the original parts. The credit card will only be charged for COBAN's list price for the part if the part has not been returned within ten (10) days.

Type of Card: _____
Credit Card Number: _____
Expiration Date: _____

OTHER INFORMATION
Unit Replacement
Once a replacement component has been received, the CLIENT must relinquish the defective unit to COBAN. If the defective unit is not returned within ten (10) days, the CLIENT agrees to pay COBAN the cost for the replacement unit upon receipt of invoice. Failure to honor the invoice within ten (10) days after receipt will cause the cancellation of this Service Description Agreement and may result in other legal actions, including but not limited to suspending shipment of subsequent units and or replacement components.

Parts Ownership
All service parts removed from the CLIENT's Supported System become the property of COBAN. The CLIENT will be obligated to pay at the current retail price(s) for any service parts removed from the CLIENT's Supported System and retained by the CLIENT. COBAN will use new and reconditioned parts made by various manufacturers in performing warranty repairs.

NON-WARRANTY SERVICES
Each warranty request pertaining to any item not covered under the EDEG Manufacture Limited Warranty shall be invoiced to the CLIENT at the agreed upon Time and Materials rate. Currently, COBAN charges $ 125.00 per hour on non-warranty phone support and $ 95.00 per hour on none warranty repair. COBAN Support Engineers are not authorized to service any third party hardware, software or vehicle issues.

COBAN will charge the CLIENT a $ 95.00 service fee for any RMA units/components that are returned to COBAN as "non-warranty" items. Non Warranty items are defined under section titled ITEMS NOT COVERED UNDER THIS WARRANTY. Non-Warranty repair work will be billed separately from this service fee.

COBAN will charge the CLIENT a $ 95.00 service fee for any RMA units/components that are returned to COBAN as "non-operational" that are in fact operational (ie: CPU units that have not been ghosted properly, scratched / hazy touch screen monitors, microphones missing parts such as: battery, internal seals, antennas, obvious misuse or damaged systems).

COBAN will obtain approval/direction for any billable service before repairs are initiated (ie. devices not covered, repairs not covered, etc)

COMPLIANCE
FAILURE TO FOLLOW ANY OF THE ABOVE INSTRUCTIONS MAY RESULT IN DELAYS AND MAY CAUSE THE CLIENT TO INCUR ADDITIONAL CHARGES, OR MAY VOID WARRANTY.

IF DURING THE REPAIR OF THE PRODUCT, THE DATA STORED ON THE HARD DRIVE ARE ALTERED, DELETED, OR IN ANY WAY MODIFIED, COBAN IS NOT RESPONSIBLE WHATSOEVER TO RECOVER OR RESTORE SAID DATA. THE CLIENT'S PRODUCT WILL BE RETURNED TO THE CLIENT IN THE ORIGINAL MANUFACTURED CONFIGURATION (SUBJECT TO AVAILABILITY OF SOFTWARE).

ITEMS NOT COVERED UNDER THIS WARRANTY
This warranty does not cover periodically or consumed parts during the life of the product such as but not limited to batteries, cables and wires; loss or damages resulting from external causes such as damaged resulting from dropping of the PRODUCT, collision with any object, fire, flooding, sand, dirt, windstorm, hail, earthquake or damage from exposure to weather conditions, misuse, abuse, damage resulting from improper use of any electrical source, power surges, damage occurring during transport.

This warranty does not cover ancillary equipment not furnished by COBAN, which may be attached to or used in connection with the PRODUCT, or for operation of the PRODUCT with any ancillary equipment. All such ancillary equipment is expressly excluded from this warranty.

All preventive maintenance recommended by COBAN to maintain the product in operating condition is the responsibility of the CLIENT; loss or damage resulting from failure to provide recommended maintenance is not covered under this contract.

- On-site service
- Triage, helpdesk phone support
- De-installation or re-installation of product(s) or software application(s)
- De-installation or re-installation of COBAN equipment performed by personnel who is not 'trained' by COBAN and/or by 'non-certified' 3rd Party installation shop.
- Warranty support or service for third party systems
- Troubleshooting of applications or application compatibility issues
- Data migration
- Vehicle related issues such as electrical
- Normal and customary wear and tear
- Damage due to connection to improper voltage supply
- PRODUCTS that has had the serial numbers removed or made illegible.

- Systems that are non operational due to abuse, neglect or improper usage for anything other than what the system was configured to do (not limited to dirt, debris, water damage or liquid of any type)
- A PRODUCT subjected to unauthorized entry or opening of the COBAN module, monitor or forced removal of the MHDD and/or components.
- A PRODUCT subjected to unauthorized PRODUCT modifications, disassemblies, or repairs (including, without limitation, the addition to the PRODUCT of non-COBAN supplied equipment) that adversely affect performance of the PRODUCT.
- Or defects or damage from improper testing, operation, maintenance, installation alteration, modification, or adjustment.
- A PRODUCT affected by virus, security breach, or other network related occurrence including but not limited to: installation of third party software applications, network security settings changes resulting in loss of communication, ability to properly use the system or configurations that deviate from the Original Master Gold Image.
- A PRODUCT, which, due to illegal or unauthorized alteration of the software / firmware in the PRODUCT, does not function in accordance with COBAN, published specifications or with the FCC type acceptance labeling in effect for the PRODUCT at the time the PRODUCT was initially distributed from COBAN.
- Scratches or other cosmetic damages to the PRODUCT's surfaces that do not affect the operation of the PRODUCT.

By installing and using the COBAN HARDWARE and SOFTWARE, CLIENT agrees to be bound by the terms of this WARRANTY STATEMENT. If CLIENT does not agree to the terms of this STATEMENT, the CLIENT should promptly contact COBAN for instruction on return of the entire PRODUCT and COBAN SOFTWARE for a refund.

FUSION HD Manufacturer Limited Warranty

(Hardware Repair Service)

The following document details the COBAN Manufacturer Limited Warranty for the FUSION HD System. COBAN Technologies, Inc. ("COBAN") warrants the COBAN Manufactured FUSION HD System ("PRODUCT"), against defects in material and workmanship under normal use and service for a period of one (1) year and, such warranties shall begin when the PRODUCT is delivered to the Original End User ("CLIENT"). This expressed Limited Warranty is extended by COBAN to the CLIENT purchasing the PRODUCT for purposes of governmental use only, and is not assignable or transferable to any other party. This is the complete warranty for the PRODUCT manufactured by COBAN and it does not warrant the installation, maintenance, support or service of the PRODUCT unless a separate written agreement is made between COBAN and CLIENT. Please refer to DVMS / Command Center Maintenance Support Service Option for technical support and software support details.

WARRANTY COVERAGE

The warranty applies within all fifty (50) states of the United States of America. This Limited Warranty is null and void if the factory applied serial number or tamper evident labels have been damaged, altered or removed from the product. COBAN, at their discretion, will at no charge, repair the PRODUCT (with new or reconditioned parts), or replace it with the same or equivalent PRODUCT (using new or reconditioned products), during the warranty period, provided that the CLIENT notifies COBAN according to the terms of this warranty. The repaired or replaced PRODUCT is warranted for the remaining original applicable warranty period. All returned parts of the PRODUCT shall become the property of COBAN.

Items covered under this warranty:

- FUSION Control Module is covered for twelve (12) months under this warranty
- FUSION Removable Pen Drive is covered for twelve (12) months under this warranty
- FUSION System Cables are covered for twelve (12) months under this warranty
- FUSION Wireless Microphone ("Mic.") Transmitter is covered for twelve (12) months under this warranty
- FUSION Wireless Mic. Receiver is covered for twelve (12) months under this warranty
- FUSION System Wires are covered for twelve (12) months under this warranty
- Wireless Mic. Transmitter Pouch is covered for twelve (12) months under this warranty
- Wireless Mic. Transmitter Battery is covered for twelve (12) months under this warranty
- Wireless Mic. Transmitter Antenna is covered for twelve (12) months under this warranty
- Wireless Mic. Receiver Antennas are covered for twelve (12) months under this warranty
- Optional Peripheral Devices are coved for twelve (12) months under this warranty

COBAN 3rd Party Warranty and Support

- Support and service on the Dell Servers and Storage is provided by Dell Computer.
  Dell Tech Support: **800-999-3355 ext 7255010** or via Website http://support.dell.com

GENERAL WARRANTY PROVISIONS

This warranty sets forth the extent of COBAN's responsibilities regarding the PRODUCT. Repair and replacement of the purchase price, at COBAN's option, is an exclusive remedy.

THE WARRANTY IS GIVEN IN LIEU OF ALL OTHER EXPRESS WARRANTIES. COBAN DISCLAIMS ALL OTHER WARRANTIES OR CONDITIONS, EXPRESSED OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL COBAN BE LIABLE FOR DAMAGES IN EXCESS OF THE ORIGINAL PURCHASE PRICE OF THE PRODUCT, FOR ANY LOSS OF USE, LOSS OF TIME, INCONVENIENCES, COMMERCIAL LOSS, LOST PROFITS, OR SAVINGS OR OTHER INCIDENTAL, SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PRODUCT TO THE FULL EXTENT THAT MAY BE DISCLAIMED BY LAW.

FORCE MAJEURE

COBAN shall not be liable for delays or failure to perform with respect to this agreement due to force majeure including (i) causes beyond the party's reasonable control and not avoidable by diligence, (ii) acts of God, epidemics, war, riots, or delays in transportation which are beyond the party's reasonable control and not avoidable by diligence, or (iii) inability for causes beyond its control and not avoidable by diligence to obtain necessary labor, materials, or manufacturing facilities, or delays caused by COBANs due to similar causes. In the event of any such delay (each such event being beyond the party's reasonable control and not avoidable by diligence), the date of performance shall be extended for a period equal to the time lost by reason of the delay.

CLIENT'S RESPONSIBILITIES
It is the CLIENT's responsibility to back up the contents of all hard drives, including any data that may be stored or software that may have been installed on the hard drive. It is possible that the contents of hard drives will be lost or that the drive may need to be reformatted in the course of service and as such COBAN will not be held liable for any damages to or loss of any program, data or other information stored on any media or any part of any PRODUCT serviced hereunder. It is HIGHLY recommended that the CLIENT create a valid disk "image" after final installation is completed. This image will need to be updated as changes are made to the units and kept safe by the CLIENT for data recovery purposes. COBAN assumes no liability or responsibility in developing a disaster recovery policy for the CLIENT. The CLIENT will perform any and ALL data reconstruction, unless specifically stated in the initial contract between COBAN and the CLIENT.

CLIENT'S REPRESENTATIVE
At all times during the term of this warranty, at least one (1) employee of the CLIENT shall be designated to act as a Representative. The Representative shall be responsible to react to all equipment problems, attempt troubleshooting to isolate the malfunction area, notify COBAN of the need for service and cooperate with COBAN to diagnose the problem over the telephone.

All initial RMA Requests MUST be called into COBAN's Tech Support line (281-925-0488 option 3) or entered via COBAN Customer Support Web Portal (http://customer.COBANTECH.com**).**
Proof of a bill of sale or purchase order (which is evidence that the PRODUCT is within the warranty period) must be presented to obtain warranty service if requested.

RMA AND SHIPPING
Once COBAN determines that all or part of the PRODUCT requires return for repair or replacement, a Return Merchandise Authorization Number (RMA NUMBER) will be issued. We recommend the CLIENT insure or get a tracking number for the return package as COBAN is not responsible for lost, stolen or damaged packages. Please prominently display the RMA number on the outside of the shipping box and ship labels of each box.

NON-WARRANTY SERVICES
Each warranty request pertaining to any item not covered under the FUSION Manufacturer Limited Warranty shall be invoiced to the CLIENT at the agreed upon time and materials rate. Currently, COBAN charges $ 125.00 per hour on non-warranty phone support and $ 95.00 per hour on non-warranty repair. COBAN Support Engineers are not authorized to service any third party hardware, software or vehicle issues.

COBAN will charge the CLIENT a $ 95.00 service fee for any RMA units/components that are returned to COBAN as "non-warranty" items. Non Warranty items are defined under section titled ITEMS NOT COVERED UNDER THIS WARRANTY. Non-Warranty repair work will be billed separately from this service fee.

COBAN will charge the CLIENT a $ 95.00 service fee for any RMA units/components that are returned to COBAN as "non-operational" that are in fact operational (ie: CPU units that have not been ghosted properly, scratched / hazy touch screen monitors, microphones missing parts such as: battery, internal seals, antennas, obvious misuse or damaged systems).

COBAN will obtain approval/direction for any billable service before repairs are initiated (ie. devices not covered, repairs not covered, etc)

COMPLIANCE
FAILURE TO FOLLOW ANY OF THE ABOVE INSTRUCTIONS MAY RESULT IN DELAYS AND MAY CAUSE THE CLIENT TO INCUR ADDITIONAL CHARGES, OR MAY VOID WARRANTY.

IF DURING THE REPAIR OF THE PRODUCT, THE DATA STORED ON THE HARD DRIVE ARE ALTERED, DELETED, OR IN ANY WAY MODIFIED, COBAN IS NOT RESPONSIBLE WHATSOEVER TO RECOVER OR RESTORE SAID DATA. THE CLIENT'S PRODUCT WILL BE RETURNED TO THE CLIENT IN THE ORIGINAL MANUFACTURED CONFIGURATION (SUBJECT TO AVAILABILITY OF SOFTWARE).

ITEMS NOT COVERED UNDER THIS WARRANTY
This warranty does not cover periodically or consumed parts during the life of the product such as but not limited to batteries, cables and wires; loss or damages resulting from external causes such as damaged resulting from dropping of the PRODUCT, collision with any object, fire, flooding, sand, dirt, windstorm, hail, earthquake or damage from

exposure to weather conditions, misuse, abuse, damage resulting from improper use of any electrical source, power surges, damage occurring during transport.

This warranty does not cover ancillary equipment not furnished by COBAN, which may be attached to or used in connection with the PRODUCT, or for operation of the PRODUCT with any ancillary equipment. All such ancillary equipment is expressly excluded from this warranty.

All preventive maintenance recommended by COBAN to maintain the product in operating condition is the responsibility of the CLIENT; loss or damage resulting from failure to provide recommended maintenance is not covered under this contract.

- On-site service
- Triage, helpdesk phone support
- De-installation or re-installation of product(s) or software application(s)
- De-installation or re-installation of COBAN equipment performed by personnel who is not 'trained' by COBAN and/or by 'non-certified' 3rd Party installation shop.
- Warranty support or service for third party systems
- Troubleshooting of applications or application compatibility issues
- Data migration
- Vehicle related issues such as electrical
- Normal and customary wear and tear
- Damage due to connection to improper voltage supply
- PRODUCTS that have had the serial numbers removed or made illegible
- Systems that are non operational due to abuse, neglect or improper usage for anything other than what the system was configured to do (not limited to dirt, debris, water damage or liquid of any type)
- A PRODUCT subjected to unauthorized entry or opening of the COBAN module, monitor or forced removal of the MHDD and/or components
- A PRODUCT subjected to unauthorized PRODUCT modifications, disassemblies, or repairs (including, without limitation, the addition to the PRODUCT of non-COBAN supplied equipment) that adversely affect performance of the PRODUCT
- Or defects or damage from improper testing, operation, maintenance, installation alteration, modification, or adjustment
- A PRODUCT affected by virus, security breach, or other network related occurrence including but not limited to: installation of third party software applications, network security settings changes resulting in loss of communication, ability to properly use the system or configurations that deviate from the Original Master Gold Image
- A PRODUCT, which, due to illegal or unauthorized alteration of the software / firmware in the PRODUCT, does not function in accordance with COBAN, published specifications or with the FCC type acceptance labeling in effect for the PRODUCT at the time the PRODUCT was initially distributed from COBAN
- Scratches or other cosmetic damages to the PRODUCT's surfaces that do not affect the operation of the PRODUCT
- By installing and using the COBAN HARDWARE and SOFTWARE, the CLIENT agrees to be bound by the terms of this WARRANTY STATEMENT. If the CLIENT does not agree to the terms of this STATEMENT, the CLIENT should promptly contact COBAN for instruction on return of the entire PRODUCT and COBAN SOFTWARE for a refund. A 15% restocking charge will be applied.

RAPID EXCHANGE OPTION Terms and Conditions – FUSION HD

The COBAN Rapid Exchange Program is an value added protection designed to minimize downtime in the event that a FUSION system needs to be repaired by COBAN service technicians. COBAN will mail qualifying agencies a replacement system, eliminating the wait time for the repair to be completed on a defective unit. The services provided by this optional plan defer to the terms of the original FUSION HD Manufacturer Limited Warranty, and only warranty-covered defects will qualify for rapid exchange.

SERVICE

It is the responsibility of the client representative to initiate the Rapid Exchange process by completing the online Return Merchandise Authorization (RMA) form (http://customer.COBANTECH.com). If the FUSION system is deemed eligible for Rapid Exchange by COBAN service technicians, a new or refurbished replacement system will be issued to the client the same day the request is processed. The client will keep the replacement, and COBAN will keep the defective module. If the defect meets the manufacturer's warranty criteria, there will be no charge to the client for the exchange.

It is the client's responsibility to back up the contents of all hard drives. It is possible that the contents of hard drives will be lost or that the drive may need to be reformatted in the course of service and as such COBAN will not be held liable for any damages to or loss of data or other information stored on any media or any part of any product returned to COBAN.

CROSS SHIPPING

Upon reviewing the RMA, COBAN service technicians will make a preliminary determination on the eligibility of the system for rapid exchange. If the system is approved, COBAN will electronically send a UPS mailing label and copy of the RMA form to the client, and immediately issue a replacement system to be shipped overnight via UPS. RMA request must be submitted by 2 p.m. Central to be processed on the same day.

The client is responsible for returning the defective unit to COBAN within ten (10) days of the replacement unit being shipped. Failure to return the system in accordance with the Rapid Exchange terms will result in the client being charged the full list price for the replacement unit.

CHARGES

Systems qualifying for rapid exchange must qualify for repair under the FUSION HD Manufacturer Limited Warranty. RMA approval does not guarantee that additional charges will not be accrued should COBAN Technical Support, upon receipt of the defective system, discover damage not covered under warranty. All information provided in the RMA must be as complete as possible to accurately determine the system's eligibility (See Non-Warranty Services, FUSION HD Manufacturer Limited Warranty). Once the system has been diagnosed by COBAN service technicians, the client will be notified of any non-warranty issues that will result in additional charges. If no such damage is found, the client's credit card will not be charged.

DVMS / Command Center Maintenance Support Services

(Phone Support and Software Support)

The following document details the COBAN DVMS / Command Center Maintenance Support Service ("SERVICE") for the EDGE, EDGE HI-DEF, TITAN M7, IP INTERVEIW ROOM SOLUTION, and DVMS / Command Center application ("PRODUCT"). COBAN Technologies, Inc. ("COBAN") offers Help Desk support and Software Maintenance to the Original End User ("CLIENT") that subscribe to this SERVICE.

SOFTWARE MAINTENANCE

As part of this SERVICE, Coban will provide software updates, service packs and /or firmware updates to the PRODUCT. Software releases that contain a chargeable new feature will not be included under this SERVICE. These features may be purchased from Coban direct. There is a target of one major releases per 12 month period (combination of software updates, service pack and/or firmware), plus as-needed patches and service packs. Service pack or firmware updates may be made available via the Coban website as a Customer downloadable and installable update. Failure to provide at least one major software update shall have no effect on the other provision of the SERVICE.

PATCHES AND UPDATES

As an industry standard best practice it is recommended, prior to applying "regular" patches / upgrades from Microsoft to the COBAN DVMS / Command Center production servers, the CLIENT shall test the patches and upgrades on a test server to ensure the integrity of the COBAN DVMS / Command Center application is not compromised, and that patches and upgrades are compatible with the CLIENT's environment and software variables. COBAN tests all such patches and upgrades internally to ensure the DVMS / Command Center application is supported by Microsoft Server on an ongoing bases.

HELPDESK SUPPORT

Maintenance Support Requests MUST be called into COBAN's Technical Support line (281-925-0488 opt.3) or entered via COBAN Customer Support Web Portal http://customer.cobantech.com (Note: the CLIENT must be a registered user to access this area.)

Maintenance Support is intended for use during business hours Monday through Friday from 8:00 AM to 6:00 PM Central Standard Time. Calls received outside of normal business hours will receive a call-back during normal business hours. Calls should be made from a location where the CLIENT's representative can physically access PRODUCT if needed during phone based troubleshooting.

CLIENT must notify COBAN within the applicable maintenance support period to obtain SERVICE. Proof of a bill of sale or purchase order (which is evidence that the PRODUCT is within the warranty period) must be presented to obtain warranty service if requested. Prior to contacting COBAN the CLIENT should have the following information on hand:

- Supported system's invoice number
- Model type
- All associated serial numbers
- Vehicles number or VIN
- Description of the problem (as well as any error messages that may be received) and any troubleshooting steps that the CLIENT has already taken.
- It is strongly recommended that the CLIENT not remove any components from the vehicle prior to contacting COBAN Support Engineers for troubleshoot.

Once the support request is accepted by the COBAN Help Desk, a Technical Support Ticket Number will be issued to the CLIENT's representative for reference and tracking purposes. CLIENT's representative will be asked to provide this ticket number to the COBAN Support Engineer in any and all communications regarding to this support request. Do not re-submit a support request if a support ticket number has already been assigned for the issue.

When requested, the CLIENT's representative will inform the COBAN Support Engineer when and what context and text of any error messages the CLIENT receives; what the CLIENT was doing when the error occurred; and what steps the CLIENT's representative may have already taken to resolve the problem. The COBAN Support Engineer will go through a series of standardized troubleshooting steps over the phone with the CLIENT's representative to help diagnose the issue. Following completion of remote troubleshooting and problem determination the COBAN Support Engineer will determine if the issue requires a RMA or if the issue can be resolved remotely over the phone.

CLIENT's representative or an authorized installation Support Engineer shall be available to assist in troubleshooting the unit by phone if needed. COBAN will contact the CLIENT's representative with this request and schedule a time to troubleshoot the unit if the appropriate personnel are not available at an appropriate time. Upon completion of troubleshooting, if the issue is not resolved, COBAN's Technical Support Department will assess the situation and determine the next course of action. Solutions to these un-resolved issues may range from issuing a Return Merchandise Authorization Number (RMA NUMBER) to having the fleet Support Engineer perform onsite repair to correct the problem. The CLIENT's representative will supply a login and connection profile for access to the CLIENT network via VPN if needed. Access will be restricted to only the server and workstation. Remote control for the server and workstation will be granted to the COBAN Support Engineer via their choice of remote access software (Terminal Services, VNC, PC Anywhere, etc).

TROUBLESHOOTING

Level 1 - The level one Help Desk is prepared to answer the most commonly asked questions, or provide resolutions that often belong in the frequently asked question or knowledge base. A Technical Support Ticket Number will be generated at the time of the initial notification of the issue (whether via phone or COBAN Customer Support Website). During the initial problem discovery and diagnostics, COBAN Support Engineers will request the CLIENT's representative to perform rudimentary troubleshooting steps. Once the issue is solved the ticket will be closed. If the issue cannot be resolved with initial call, the COBAN Support Engineer will escalate the issue to a level 2 Help Desk for further research/troubleshooting.

Level 2 - The level two Help Desk will require servicing/repairing on the components (i.e. camera, CPU, power supply, etc.) If service or repair is required, a COBAN Support Engineer will issue a RMA Number and instruct the CLIENT's representative to return the defective components to COBAN. Prior to issuing an RMA Number for the component, the COBAN Support Engineer may request that the in-car unit be "re-imaged" by the CLIENT's representative to see if this resolves the matter. If a re-image process and components replacement does not resolve the issue, the problem will be escalated to a Level 3 Help Desk. Cross ship or unit replacement will be issued at COBAN's discretion.

Level 3 - Level three issues are typically classified as "Total System Failures" meaning the system is not operational or useable by the CLIENT. If this is the case, and the serviced or repaired components did not resolve the issue, a complete system replacement will be sent (if that is determined to be the only solution.) Additional troubleshooting and diagnostics will be attempted prior to issuing an RMA for a complete system replacement or the vehicle may need to be sent to the authorized service center for diagnostics test. Initial response time after COBAN escalates a problem to this level is four (4) to eight (8) business hours. Resolution times will vary depending on the nature of the problem.

Coban 3rd Party Warranty and Support

- Support and service on the Rimage Auto DVD Burner is provided by QUMU Product

Rimage Support: **1-800-553-8312 ext. 2** or via Website https://rimagesupport.qumu.com/hc/en-us/requests/new

- Support and service on VieVu LE2 and LE3 is provided by VieVu

Dell Tech Support: **1-800-999-3355 ext. 7255010** or via Website http://support.dell.com

- Support and service on the IBM Server, Storage, Tape Library and Tivoli Storage Manager Software is provided by IBM. IBM Support: **1800-426-7378** or via Website http://www.ibm.com/support/us/en/

CLIENT'S REPRESENTATIVE

At all times during the term of this SERVICE, at least one (1) employee of the CLIENT shall be designated to act as Representative. Representative shall be responsible to react to all equipment problems, attempt troubleshoot to isolate the malfunction area, apply patches and updates that are supplied by Coban, notify Coban of the need for support and cooperate with Coban to diagnose the problem over the telephone.

CLIENTS RESPONSIBILITY

It is the CLIENT's responsibility to backup the contents of all hard drives, including any data that may be stored or software that may have been installed on the hard drive. It is possible that the contents of hard drives will be lost or that the drive may need to be reformatted in the course of service and as such COBAN will not be held liable for any damage to or loss of any program, data or other information stored on any media or any part of any PRODUCT serviced hereunder. It is HIGHLY recommended that the CLIENT create a valid disk "image" after final installation is completed. This image will need to be updated as changes are made to the units and kept safe by the CLIENT for data recovery purposes. COBAN assumes no liability or responsibility in developing a disaster recovery policy for the CLIENT. The CLIENT will perform any and ALL data reconstruction, unless specifically stated in the initial contract between COBAN and the CLIENT. COBAN shall not be liable for delays or failure to perform with respect to this agreement due to Force Majeure including (i) causes beyond the party's reasonable control and not avoidable by diligence, (ii) acts of God, epidemics, war, riots, or delays in transportation which are beyond the party's reasonable control and not avoidable by diligence, or (iii) inability for causes beyond its control and not avoidable by diligence to

obtain necessary labor, materials, or manufacturing facilities, or delays caused by COBANs due to similar causes. In the event of any such delay (each such event being beyond the party's reasonable control and not avoidable by diligence), the date of performance shall be extended for a period equal to the time lost by reason of the delay.

CLIENT will respond to request for information including but not limited to the PRODUCT serial number, model, version of the operating system and software installed, any peripherals devices connected or installed on the PRODCUT, any error messages displayed actions taken before the PRODUCT experienced the issue and steps take to resolve the issue.

ITEMS NOT COVERED UNDER THIS MAINTENANCE SUPPORT SERVICE

Each support request, repair or troubleshooting pertaining to any item not covered under this SERVICE shall be invoiced to the CLIENT at the agreed upon Time and Materials rate. Currently, COBAN charges $125.00 per hour on non-warranty phone support and $ 95.00 per hour on none warranty repair. COBAN Support Engineers are not authorized to service any third party hardware, software or vehicle issues.

- On-site service
- Install or apply patches
- Warranty support or service for third party hardware or application
- Operating system or driver updates
- Re-mastering of the Fusion, EDGE or TITAN images
- Data migration
- PRODUCTS that has had the serial numbers removed or made illegible
- Systems that are nonoperational due to abuse, neglect or improper usage for anything other than what the system was configured to do (not limited to dirt, debris, water damage or liquid of any type)
- A PRODUCT subjected to unauthorized entry or opening of the COBAN module, monitor or forced removal of the MHDD and/or components
- A PRODUCT subjected to unauthorized PRODUCT modifications, disassembly, or repairs (including, without limitation, the addition to the PRODUCT of non-COBAN supplied equipment) that adversely affect performance of the PRODUCT
- Or defects or damage from improper testing, operation, maintenance, installation alteration, modification, or adjustment
- A PRODUCT affected by virus, security breach, or other network related occurrence including but not limited to: installation of third party software applications, network security settings changes resulting in loss of communication, ability to properly use the system or configurations that deviate from the Original Master Gold Image
- A PRODUCT, which, due to illegal or unauthorized alteration of the software / firmware in the PRODUCT, does not function in accordance with COBAN, published specifications or with the FCC type acceptance labeling in effect for the PRODUCT at the time the PRODUCT was initially distributed from COBAN
- Scratches or other cosmetic damages to the PRODUCT’s surfaces that do not affect the operation of the PRODUCT

By installing and using the COBAN HARDWARE and SOFTWARE, the CLIENT agrees to be bound by the terms of this WARRANTY STATEMENT.

Software License

GRANT OF LICENSE
Copyright laws and international copyright treaties, as well as other intellectual property laws and treaties protect the COBAN SOFTWARE. The COBAN SOFTWARE is licensed, not sold.
This LICENSE grants CLIENT the following rights:

- **Software.** CLIENT may install and use one copy of the COBAN SOFTWARE on the PRODUCT
- **Storage/Network Use.** CLIENT may install the DVMS / Command Center CLIENT software on their existing internal local area network. The CLIENT may not make unauthorized copies of the COBAN Mobile Start software without the express written consent of COBAN. COBAN assumes no liability for software installation failures due to incompatible hardware, software or network security issues that are controlled by the CLIENT Information Technology Department. COBAN will not be responsible to install said software on the CLIENT local area network, unless specifically contracted to do so. Instructions shall be provided to the CLIENT to accomplish this task.
- **Back-up Copy.** A back-up copy of the COBAN SOFTWARE is included with the PRODUCT. CLIENT may use the back-up copy solely for archival purpose.

DESCRIPTION OF OTHER RIGHTS & LIMITATION

- **Limitation on Reverse Engineering.** De-compilation and Disassembly. CLIENT may not modify, reverse engineer, de-compile, or disassemble the COBAN SOFTWARE or HARDWARE in whole or in part without the express consent from COBAN. Failure to obtain consent may void any and all warranties.
- **Separation of Components.** The COBAN SOFTWARE is licensed as a single product. Its component parts may not be separated for use on more than one PRODUCT.
- **Single PRODUCT.** The COBAN SOFTWARE is licensed with the PRODUCT as a single integrated product. The COBAN SOFTWARE may only be used with the PRODUCT.
- **Rental.** CLIENT may not rent or lease the COBAN SOFTWARE.
- **Software Transfer.** Software / Hardware / Licenses are NOT transferable.
- **Termination.** Without prejudice to any other rights, COBAN may terminate this LICENSE if the CLIENT fails to comply with the terms and conditions of this LICENSE. In such event, the CLIENT must destroy all copies of the COBAN SOFTWARE and all of its component parts.

PROHIBITION ON EXPORTATION
EXCEPT FOR EXPORT TO CANADA AND AUSTRALIA, THE COBAN SOFTWARE AND ANY UNDERLYING TECHNOLOGY MAY NOT BE EXPORTED OUTSIDE THE UNITED STATES OR TO ANY FOREIGN ENTITY OR "FOREIGN PERSON" AS DEFINED BY U.S. GOVERNMENT REGULATION, INCLUDING WITHOUT LIMITATION, ANYONE WHO IS NOT A CITIZEN, OR LAWFUL PERMANENT RESIDENT OF THE UNITED STATES. CLIENT AGREES THAT BY DOWNLOADING OR USING THE COBAN SOFTWARE, THEY ARE AGREEING TO THE FOREGOING AND THEY ARE WARRANTING THAT THEY ARE NOT A "FOREIGN PERSON" OR UNDER THE CONTROL OF OR ACTING ON BEHALF OF THE FOREIGN ENTITY.

U.S. GOVERNMENT RESTRICTED RIGHTS
The Software Product and documentation are provided with RESTRICTED RIGHTS. Use, duplication, or disclosure by the United State Government is subject to restrictions as set forth in subparagraph (c)(1) and (2) of the Commercial PRODUCT Software-Restricted Rights at 48 CFR 52.227-19, as applicable. Manufacturer is COBAN Technologies, Inc., 11375 W Sam Houston Parkway S # 800, Houston, TX 77031.

SOFTWARE WARRANTIES - Reserved
The COBAN PRODUCT described in this instruction manual may include copyrighted COBAN SOFTWARE stored in semiconductor memory and other media. Laws in the United States and other countries preserve certain exclusive rights for COBAN copyrighted SOFTWARE programs, including the exclusive right to copy or reproduce the copyrighted SOFTWARE program in any form. Accordingly, any copyrighted COBAN SOFTWARE programs contained in the COBAN PRODUCT described in this instruction manual may not be copied or reproduced in any manner without the express written permission of COBAN. Furthermore, the CLIENT shall not be deemed to grant either directly or by implication, estoppels or otherwise, any license under the copyrights, patents or patent applications for COBAN, except for the normal non-exclusive, royalty-free license to use that arises by operation of law in the sale of a product.

END USER LICENSE AGREEMENT
This End-User License Agreement ("LICENSE") is a legal agreement between the CLIENT and COBAN Technologies, Inc. ("COBAN"), the manufacturer of the EDGE, EDGE HI-DEF, TITAN M7, IP INTERVEIW ROOM SOLUTION ("PRODUCT"). All COBAN software, including COBAN Mobile Start Software ("SOFTWARE") and third party software not otherwise licensed by a specific end user license agreement included with CLIENT PRODUCT, downloaded from

COBAN websites or provided by COBAN as update / upgrades, shall be referred to as COBAN SOFTWARE. The COBAN SOFTWARE includes PRODUCT software, the associated media, any printed materials, and any “on-line” or electronic documentation, as well as COBAN supplied or facilitated update / upgrades thereto. Notwithstanding for foregoing, software distributed together with separate end user software license agreements (the “Third Party EULA”), including but not limited to Windows® operating system provided by Microsoft Corporation, shall be covered by respective Third Party EULAs. CLIENT may use the COBAN SOFTWARE only in connection with the use of PRODUCT. By installing, copying, downloading or otherwise using the COBAN SOFTWARE, CLIENT agrees to be bound by the terms of this LICENSE. If CLIENT does not agree to the terms of this LICENSE, the CLIENT should promptly contact COBAN for instruction on return of the entire PRODUCT and COBAN SOFTWARE for a refund. A 15% restocking charge will be applied.

11375 West Sam Houston Parkway South # 800
Houston, Texas 77031

FUSION HD RAPID EXCHANGE OPTION

Terms and Conditions

The COBAN Rapid Exchange Program is designed to minimize downtime in the event that a FUSION system needs to be repaired by COBAN service technicians. COBAN will mail qualifying agencies a replacement system, eliminating the wait time for the repair to be completed on a defective unit. The services provided by this optional plan defer to the terms of the original FUSION HD Manufacturer Limited Warranty, and only warranty-covered defects will qualify for rapid exchange.

Service

It is the responsibility of the client representative to initiate the Rapid Exchange process by completing the online Return Merchandise Authorization (RMA) form (http://customer.COBANTECH.com). If the FUSION system is deemed eligible for Rapid Exchange by COBAN service technicians, a new or refurbished replacement system will be issued to the client the same day the request is processed. The client will keep the replacement, and COBAN will keep the defective module. If the defect meets the manufacturer's warranty criteria, there will be no charge to the client for the exchange.

It is the client's responsibility to back up the contents of all hard drives. It is possible that the contents of hard drives will be lost or that the drive may need to be reformatted in the course of service and as such COBAN will not be held liable for any damages to or loss of data or other information stored on any media or any part of any product returned to COBAN.

Cross-Shipping

Upon reviewing the RMA, COBAN service technicians will make a preliminary determination on the eligibility of the system for rapid exchange. If the system is approved, COBAN will electronically send a UPS mailing label and copy of the RMA form to the client, and immediately issue a replacement system to be shipped overnight via UPS. RMA request must be submitted by 2 p.m. Central to be processed on the same day.

The client is responsible for returning the defective unit to COBAN within ten (10) days of the replacement unit being shipped. Failure to return the system in accordance with the Rapid Exchange terms will result in the client being charged the full list price for the replacement unit.

Charges

Systems qualifying for rapid exchange must qualify for repair under the FUSION HD Manufacturer Limited Warranty. RMA approval does not guarantee that additional charges will not be accrued should COBAN Technical Support, upon receipt of the defective system, discover damage not covered under warranty. All information provided in the RMA must be as complete as possible to accurately determine the system's eligibility (See Non-Warranty Services, FUSION HD Manufacturer Limited Warranty). Once the system has been diagnosed by COBAN service technicians, the client will be notified of any non-warranty issues that will result in additional charges. If no such damage is found, the client's credit card will not be charged.

DVMS / Command Center Maintenance Support Services

(Phone Support and Software Support)

The following document details the COBAN DVMS / Command Center Maintenance Support Service ("SERVICE") for the Body Worn Camera and DVMS / Command Center application ("PRODUCT"). COBAN Technologies, Inc. ("COBAN") offers Help Desk support and Software Maintenance to the Original End User ("CLIENT") that subscribe to this SERVICE.

SOFTWARE MAINTENANCE

As part of this SERVICE, COBAN will provide software updates, service packs and /or firmware updates to the PRODUCT. Software releases that contain a chargeable new feature will not be included under this SERVICE. These features may be purchased from COBAN directly. There is a target of one major releases per 12 month period (combination of software updates, service pack and/or firmware), plus as-needed patches and service packs. Service pack or firmware updates may be made available via the Coban website as a Customer downloadable and installable update. Failure to provide at least one major software update shall have no effect on the other provision of the SERVICE.

PATCHES AND UPDATES

As an industry standard best practice it is recommended, prior to applying "regular" patches / upgrades from Microsoft to the COBAN DVMS / Command Center production servers, the CLIENT shall test the patches and upgrades on a test server to ensure the integrity of the COBAN DVMS / Command Center application is not compromised, and that patches and upgrades are compatible with the CLIENT's environment and software variables. COBAN tests all such patches and upgrades internally to ensure the DVMS / Command Center application is supported by Microsoft Server on an ongoing bases.

HELPDESK SUPPORT

Maintenance Support Requests MUST be called into COBAN's Technical Support line (281-925-0488 opt.3) or entered via COBAN Customer Support Web Portal http://customer.cobantech.com (Note: the CLIENT must be a registered user to access this area.)

Maintenance Support is intended for use during business hours Monday through Friday from 8:00 AM to 6:00 PM Central Standard Time. Calls received outside of normal business hours will receive a call-back during normal business hours. Calls should be made from a location where the CLIENT's representative can physically access PRODUCT if needed during phone based troubleshooting.

CLIENT must notify COBAN within the applicable maintenance support period to obtain SERVICE. Proof of a bill of sale or purchase order (which is evidence that the PRODUCT is within the warranty period) must be presented to obtain warranty service if requested. Prior to contacting COBAN the CLIENT should have the following information on hand:

- Supported system's invoice number
- Model type
- All associated serial numbers
- Vehicles number or VIN
- Description of the problem (as well as any error messages that may be received) and any troubleshooting steps that the CLIENT has already taken.
- It is strongly recommended that the CLIENT not remove any components from the vehicle prior to contacting COBAN Support Engineers for troubleshoot.

Once the support request is accepted by the COBAN Help Desk, a Technical Support Ticket Number will be issued to the CLIENT's representative for reference and tracking purposes. CLIENT's representative will be asked to provide this ticket number to the COBAN Support Engineer in any and all communications regarding to this support request. Do not re-submit a support request if a support ticket number has already been assigned for the issue.

When requested, the CLIENT's representative will inform the COBAN Support Engineer when and what context and text of any error messages the CLIENT receives; what the CLIENT was doing when the error occurred; and what steps the CLIENT's representative may have already taken to resolve the problem. The COBAN Support Engineer will go through a series of standardized troubleshooting steps over the phone with the CLIENT's representative to help diagnose the issue. Following completion of remote troubleshooting and problem

determination the COBAN Support Engineer will determine if the issue requires a RMA or if the issue can be resolved remotely over the phone.

CLIENT's representative or an authorized installation Support Engineer shall be available to assist in troubleshooting the unit by phone if needed. COBAN will contact the CLIENT's representative with this request and schedule a time to troubleshoot the unit if the appropriate personnel are not available at an appropriate time. Upon completion of troubleshooting, if the issue is not resolved, COBAN's Technical Support Department will assess the situation and determine the next course of action. Solutions to these un-resolved issues may range from issuing a Return Merchandise Authorization Number (RMA NUMBER) to having the fleet Support Engineer perform onsite repair to correct the problem. The CLIENT's representative will supply a login and connection profile for access to the CLIENT network via VPN if needed. Access will be restricted to only the server and workstation. Remote control for the server and workstation will be granted to the COBAN Support Engineer via their choice of remote access software (Terminal Services, VNC, PC Anywhere, etc).

TROUBLESHOOTING

Level 1 - The level one Help Desk is prepared to answer the most commonly asked questions, or provide resolutions that often belong in the frequently asked question or knowledge base. A Technical Support Ticket Number will be generated at the time of the initial notification of the issue (whether via phone or COBAN Customer Support Website). During the initial problem discovery and diagnostics, COBAN Support Engineers will request the CLIENT's representative to perform rudimentary troubleshooting steps. Once the issue is solved the ticket will be closed. If the issue cannot be resolved with initial call, the COBAN Support Engineer will escalate the issue to a level 2 Help Desk for further research/troubleshooting.

Level 2 - The level two Help Desk will require servicing/repairing on the components (i.e. camera, CPU, power supply, etc.) If service or repair is required, a COBAN Support Engineer will issue a RMA Number and instruct the CLIENT's representative to return the defective components to COBAN. Prior to issuing an RMA Number for the component, the COBAN Support Engineer may request that the in-car unit be "re-imaged" by the CLIENT's representative to see if this resolves the matter. If a re-image process and components replacement does not resolve the issue, the problem will be escalated to a Level 3 Help Desk. Cross ship or unit replacement will be issued at COBAN's discretion.

Level 3 - Level three issues are typically classified as "Total System Failures" meaning the system is not operational or useable by the CLIENT. If this is the case, and the serviced or repaired components did not resolve the issue, a complete system replacement will be sent (if that is determined to be the only solution.) Additional troubleshooting and diagnostics will be attempted prior to issuing an RMA for a complete system replacement or the vehicle may need to be sent to the authorized service center for diagnostics test. Initial response time after COBAN escalates a problem to this level is four (4) to eight (8) business hours. Resolution times will vary depending on the nature of the problem.

Coban 3rd Party Warranty and Support

- Support and service on the Rimage Auto DVD Burner is provided by QUMU Product
  Rimage Support: **1-800-553-8312 ext. 2** or via Website https://rimagesupport.qumu.com/hc/en-us/requests/new
- Support and service on the Dell Servers and Storage is provided by Dell Computer
  Dell Tech Support: **1-800-3355 ext. 7255010** or via Website http://support.dell.com
- Support and service on the IBM Server, Storage, Tape Library and Tivoli Storage Manager Software is provided by IBM. IBM Support: **1800-426-7378** or via Website http://www.ibm.com/support/us/en/

CLIENT'S REPRESENTATIVE

At all times during the term of this SERVICE, at least one (1) employee of the CLIENT shall be designated to act as Representative. Representative shall be responsible to react to all equipment problems, attempt troubleshoot to isolate the malfunction area, apply patches and updates that are supplied by Coban, notify Coban of the need for support and cooperate with Coban to diagnose the problem over the telephone.

CLIENTS RESPONSIBILITY

It is the CLIENT's responsibility to backup the contents of all hard drives, including any data that may be stored or software that may have been installed on the hard drive. It is possible that the contents of hard drives will be lost or that the drive may need to be reformatted in the course of service and as such COBAN will not be held liable for any damage to or loss of any program, data or other information stored on any media or any part of any PRODUCT serviced hereunder. It is HIGHLY recommended that the CLIENT create a valid disk "image" after final installation is completed. This image will need to be updated as changes are made to the units and kept safe by

the CLIENT for data recovery purposes. COBAN assumes no liability or responsibility in developing a disaster recovery policy for the CLIENT. The CLIENT will perform any and ALL data reconstruction, unless specifically stated in the initial contract between COBAN and the CLIENT. COBAN shall not be liable for delays or failure to perform with respect to this agreement due to Force Majeure including (i) causes beyond the party's reasonable control and not avoidable by diligence, (ii) acts of God, epidemics, war, riots, or delays in transportation which are beyond the party's reasonable control and not avoidable by diligence, or (iii) inability for causes beyond its control and not avoidable by diligence to obtain necessary labor, materials, or manufacturing facilities, or delays caused by COBANs due to similar causes. In the event of any such delay (each such event being beyond the party's reasonable control and not avoidable by diligence), the date of performance shall be extended for a period equal to the time lost by reason of the delay.

CLIENT will respond to request for information including but not limited to the PRODUCT serial number, model, version of the operating system and software installed, any peripherals devices connected or installed on the PRODCUT, any error messages displayed actions taken before the PRODUCT experienced the issue and steps take to resolve the issue.

ITEMS NOT COVERED UNDER THIS MAINTENANCE SUPPORT SERVICE

Each support request, repair or troubleshooting pertaining to any item not covered under this SERVICE shall be invoiced to the CLIENT at the agreed upon Time and Materials rate. Currently, COBAN charges $125.00 per hour on non-warranty phone support and $ 95.00 per hour on none warranty repair. COBAN Support Engineers are not authorized to service any third party hardware, software or vehicle issues.

- On-site service
- Install or apply patches
- Warranty support or service for third party hardware or application.
- Operating system or driver updates
- Data migration
- PRODUCTS that has had the serial numbers removed or made illegible.
- Systems that are nonoperational due to abuse, neglect or improper usage for anything other than what the system was configured to do (not limited to dirt, debris, water damage or liquid of any type)
- A PRODUCT subjected to unauthorized entry or opening of the COBAN module, monitor or forced removal of the MHDD and/or components.
- A PRODUCT subjected to unauthorized PRODUCT modifications, disassembly, or repairs (including, without limitation, the addition to the PRODUCT of non-COBAN supplied equipment) that adversely affect performance of the PRODUCT.
- Or defects or damage from improper testing, operation, maintenance, installation alteration, modification, or adjustment.
- A PRODUCT affected by virus, security breach, or other network related occurrence including but not limited to: installation of third party software applications, network security settings changes resulting in loss of communication, ability to properly use the system or configurations that deviate from the Original Master Gold Image.
- A PRODUCT, which, due to illegal or unauthorized alteration of the software / firmware in the PRODUCT, does not function in accordance with COBAN, published specifications or with the FCC type acceptance labeling in effect for the PRODUCT at the time the PRODUCT was initially distributed from COBAN.
- Scratches or other cosmetic damages to the PRODUCT’s surfaces that do not affect the operation of the PRODUCT.

By installing and using the Body Worn Camera and SOFTWARE, CLIENT agrees to be bound by the terms of this WARRANTY STATEMENT.

Software License

GRANT OF LICENSE

Copyright laws and international copyright treaties, as well as other intellectual property laws and treaties protect the COBAN SOFTWARE. The COBAN SOFTWARE is licensed, not sold.

This LICENSE grants CLIENT the following rights:

- **Software.** CLIENT may install and use one copy of the COBAN SOFTWARE on the PRODUCT
- **Storage/Network Use.** CLIENT may install the DVMS / Command Center CLIENT software on their existing internal local area network. The CLIENT may not make unauthorized copies of the COBAN Mobile Start software without the express written consent of COBAN. COBAN assumes no liability for software installation failures due to incompatible hardware, software or network security issues that are controlled by the CLIENT Information Technology Department. COBAN will not be responsible to install said software on the CLIENT local area network, unless specifically contracted to do so. Instructions shall be provided to the CLIENT to accomplish this task.
- **Back-up Copy.** A back-up copy of the COBAN SOFTWARE is included with the PRODUCT. CLIENT may use the back-up copy solely for archival purpose.

DESCRIPTION OF OTHER RIGHTS & LIMITATION

- **Limitation on Reverse Engineering.** De-compilation and Disassembly. CLIENT may not modify, reverse engineer, de-compile, or disassemble the COBAN SOFTWARE or HARDWARE in whole or in part without the express consent from COBAN. Failure to obtain consent may void any and all warranties.
- **Separation of Components.** The COBAN SOFTWARE is licensed as a single product. Its component parts may not be separated for use on more than one PRODUCT.
- **Single PRODUCT.** The COBAN SOFTWARE is licensed with the PRODUCT as a single integrated product. The COBAN SOFTWARE may only be used with the PRODUCT.
- **Rental.** CLIENT may not rent or lease the COBAN SOFTWARE.
- **Software Transfer.** Software / Hardware / Licenses are NOT transferable.
- **Termination.** Without prejudice to any other rights, COBAN may terminate this LICENSE if the CLIENT fails to comply with the terms and conditions of this LICENSE. In such event, the CLIENT must destroy all copies of the COBAN SOFTWARE and all of its component parts.

PROHIBITION ON EXPORTATION

EXCEPT FOR EXPORT TO CANADA AND AUSTRALIA, THE COBAN SOFTWARE AND ANY UNDERLYING TECHNOLOGY MAY NOT BE EXPORTED OUTSIDE THE UNITED STATES OR TO ANY FOREIGN ENTITY OR "FOREIGN PERSON" AS DEFINED BY U.S. GOVERNMENT REGULATION, INCLUDING WITHOUT LIMITATION, ANYONE WHO IS NOT A CITIZEN, OR LAWFUL PERMANENT RESIDENT OF THE UNITED STATES. CLIENT AGREES THAT BY DOWNLOADING OR USING THE COBAN SOFTWARE, THEY ARE AGREEING TO THE FOREGOING AND THEY ARE WARRANTING THAT THEY ARE NOT A "FOREIGN PERSON" OR UNDER THE CONTROL OF OR ACTING ON BEHALF OF THE FOREIGN ENTITY.

U.S. GOVERNMENT RESTRICTED RIGHTS

The Software Product and documentation are provided with RESTRICTED RIGHTS. Use, duplication, or disclosure by the United State Government is subject to restrictions as set forth in subparagraph (c)(1) and (2) of the Commercial PRODUCT Software-Restricted Rights at 48 CFR 52.227-19, as applicable. Manufacturer is COBAN Technologies, Inc., 12503 Exchange Drive, Suite 536, Stafford, Texas 77477.

SOFTWARE WARRANTIES - Reserved

The COBAN PRODUCT described in this instruction manual may include copyrighted COBAN SOFTWARE stored in semiconductor memory and other media. Laws in the United States and other countries preserve certain exclusive rights for COBAN copyrighted SOFTWARE programs, including the exclusive right to copy or reproduce the copyrighted SOFTWARE program in any form. Accordingly, any copyrighted COBAN SOFTWARE programs contained in the COBAN PRODUCT described in this instruction manual may not be copied or reproduced in any manner without the express written permission of COBAN. Furthermore, the CLIENT shall not be deemed to grant either directly or by implication, estoppels or otherwise, any license under the copyrights, patents or patent applications for COBAN, except for the normal non-exclusive, royalty-free license to use that arises by operation of law in the sale of a product.

END USER LICENSE AGREEMENT

This End-User License Agreement ("LICENSE") is a legal agreement between the CLIENT and COBAN Technologies, Inc. ("COBAN"), the manufacturer of the TOPCAM, TOPCAM-PV, VMDT G-II, MDT, MDT-PV and TOPCAM Systems ("PRODUCT"). All COBAN software, including COBAN Mobile Start Software ("SOFTWARE")

and third party software not otherwise licensed by a specific end user license agreement included with CLIENT PRODUCT, downloaded from COBAN websites or provided by COBAN as update / upgrades, shall be referred to as COBAN SOFTWARE. The COBAN SOFTWARE includes PRODUCT software, the associated media, any printed materials, and any “on-line” or electronic documentation, as well as COBAN supplied or facilitated update / upgrades thereto. Notwithstanding for foregoing, software distributed together with separate end user software license agreements (the “Third Party EULA”), including but not limited to Windows® operating system provided by Microsoft Corporation, shall be covered by respective Third Party EULAs. CLIENT may use the COBAN SOFTWARE only in connection with the use of PRODUCT. By installing, copying, downloading or otherwise using the COBAN SOFTWARE, CLIENT agrees to be bound by the terms of this LICENSE.

COBAN Technologies, Inc.
Support and Subscription Services "SnS" Terms and Conditions

(For On-Premise Software and Hardware Products)

COBAN Technologies, Inc., a Texas corporation, as applicable (**"COBAN"**), shall provide Technical Support and Subscription Services (as defined herein) (collectively, the **"Services")** to the Customer, per the terms of this Agreement (the "**Agreement**") and as set forth at the COBAN Support Services Website, at http://www.COBANTECH.com/support/services/ . The applicable COBAN entity, **Effective Date**, **Software**, and Services level will be set forth on the applicable enterprise license agreement, SnS order form, Customer's purchase Order, or, if Customer has purchased support on a per-incident basis (**"Per Incident"**), in the registration form completed by Customer upon such purchase (collectively the **"Order"**).

1. Definitions.

1.1 "**Error**" means a failure in the Software to materially conform to the specifications described in the applicable product documentation ("**Documentation**").

1.2 "**Modified Code**" means any modification, addition and/or development of code scripts deviating from the predefined product code tree(s)/modules developed by COBAN for production deployment or use. Modified Code excludes customizable Software options for which COBAN offers Services on the applicable COBAN price list.

1.3 "**Services Fees**" means the fees for Services specified in a corresponding COBAN or reseller invoice.

1.4 "**Services Period**" means the period for which Customer has purchased the Services and any subsequent renewal periods and shall commence: (a) for Software Licenses for which Services are mandatory, on the date the applicable Software License Key(s) are made available for download, and (b) for Software Licenses for which Services are optional, on the date of purchase of the Services.

1.5 "**Severity**" is a measure of the relative impact an Error has on the use of the Software, as defined by COBAN, and assigned by Customer when opening a Support request. The following Severity levels apply to all Software:

> **(a)** "**Severity One**" means Customer's production server or other mission critical system(s) are down and no workaround is immediately available and (i) all or a substantial portion of Customer's mission critical data is at a significant risk of loss or corruption; (ii) Customer has had a substantial loss of service; or (iii) Customer's business operations have been severely disrupted.
>
> **(b)** "**Severity Two**" means that major functionality is severely impaired such that (i) operations can continue in a restricted fashion, although long-term productivity might be adversely affected; (ii) a major milestone is at risk; ongoing and incremental installations are affected; or (iii) only a temporary workaround is available. Severity Two includes assistance with retrieval of failsave videos for critical incidents.
>
> **(c)** "**Severity Three**" means a partial, non-critical loss of functionality of the software or hardware such that: (i) the operation of some component(s) is impaired but allows the user to continue using the Software and other available in-car cameras, body worn cameras, and/or interview room cameras; or (ii) initial installation milestones are at minimal risk.
>
> **(d)** "**Severity Four**" means general usage questions and cosmetic issues, including errors in the Documentation.

1.6 "**Software**" means software offered on the COBAN price list, and all components shipped with the Software, including Open Source components.

1.7 "**Subscription Services**" means the provision of Maintenance Releases, Minor Releases and Major Releases (each defined below), if any, to the Software, as well as corresponding Documentation, to Customer.

(a) "**Maintenance Release**" or "**Update**" means a generally available release of the Software that typically provides maintenance corrections only or high severity bug fixes, designated by COBAN by means of a change in the digit to the right of the second decimal point (e.g. Software 5.0 >> Software 5.0.1).

(b) "**Minor Release**" means a generally available release of the Software that (i) introduces a limited amount of new features, functionality and minor enhancements; (ii) fixes for high severity and high priority bugs identified in the current release, and (iii) is designated by COBAN by means of a change in the digit to the right of the decimal point (e.g., Software 5.0>>Software 5.1).

(c) "**Major Release,**" also known as an "**Upgrade,**" means a generally available release of the Software that (i) contains functional enhancements and extensions, (ii) fixes for high severity and high priority bugs, and (iii) is designated by COBAN by means of a change in the digit to the left of the first decimal point (e.g., Software 5.0 >> Software 6.0).

1.8 "**Technical Support**" means the provision of telephone or web-based technical assistance by COBAN to Customer's technical contact(s) with respect to installation, Errors and technical product problems, at the corresponding Services level purchased by Customer.

1.9 "**Third Party Products**" means any software or hardware that is manufactured by a party other than COBAN and is either: (i) not delivered with the Software; or (ii) not incorporated into the Software.

2. Service Terms.

2.1 Provision of Services. Subject to the terms of this Agreement, COBAN shall, during the Services Period, provide Customer with Services at the applicable Services level purchased.

2.2 End of Availability. COBAN may, at its discretion, decide to retire Software and/or Services from time to time ("**End of Availability**"). COBAN shall publicly post for all customers notice of End of Availability, including the last date of general commercial availability of the affected Software and the timeline for discontinuing Services, at https://www.COBAN.com/support/policies/lifecycle.html. COBAN shall have no obligation to provide Services for Software that is outside of the applicable Service life.

2.3 Purchase Requirements.

(a) Except as otherwise provided for by COBAN, Customer may purchase initial Services only for the most current, generally available release of the Software.

(b) Customer must purchase and/or renew Services at the same Services level for all of the licenses for a particular Software product or suite that has been installed in a given environment, such as Test, Development, QA, or Production (i.e. Customer cannot purchase Production level support for only one license per unit in its lab and purchase Basic level support for the other units in that environment).

(c) Except as otherwise provided in the applicable price list, the minimum term for any Service offering is one (1) year.

(d) These Services Terms and conditions will automatically update to COBAN's then-current Services terms and conditions set forth at https://www.COBANTECH.com/files/pdf/support/support_terms_conditions.pdf upon any renewal of Services.

2.4 Exclusions.

(a) Services do not cover problems caused by the following:

(i) unusual external physical factors such as inclement weather conditions that cause electrical or electromagnetic stress or a failure of electric power, air conditioning or humidity control; neglect; misuse; operation of the Software with other media not in accordance with the manufacturer's specifications; or causes other than ordinary use;

(ii) use of the Software that deviates from any operating procedures as specified in the Documentation;

(iii) Third Party Products, other than the interface of the Software with the Third Party Products;

(iv) Modified Code;

(v) issues relating to Software offered as a Service ("SaaS"), or other "X"aaS offerings;

(vi) any customized deliverables created by COBAN, COBAN partners or third-party service providers specifically for Customer as part of consulting services;

(vii); use of the Software with unsupported tools (i.e., Java Development Kit (JDK); Java Runtime Environment (JRE)), APIs, interfaces or data formats other than those included with the Software and supported as set forth in the Documentation. Customer may request assistance from COBAN for such problems, for an additional fee.

(b) In the event that COBAN suspects that a reported problem may be related to Modified Code or 3rd Party Product, COBAN, may, in its sole discretion,

(i) request that the Modified Code or 3rd Party Product be removed, and/or

(ii) inform Customer that additional assistance may be obtained by Customer directly from various product discussion forums or by engaging COBAN's consulting services group for an additional fee.

2.5 Customer Responsibilities. COBAN's obligations regarding Services are subject to the following:

(a) Customer agrees to receive from COBAN communications via e-mail, telephone, and other formats, regarding Services (such as communications concerning support coverage, Errors or other technical issues and the availability of new releases of the Software and training options).

(b) Customer's technical contact shall cooperate to enable COBAN to deliver the Services.

(c) Customer is solely responsible for the use of the Software by its personnel and shall properly train its personnel in the use and application of the Software.

(d) Customer shall promptly report to COBAN all problems with the Software, and shall implement any corrective procedures provided by COBAN reasonably promptly after receipt.

(e) Customer is solely responsible for protecting and backing up the data and information stored on the computers on which the Software is used and should confirm that such data and information is protected and backed up in accordance with any internal or regulatory requirements as applicable, before contacting COBAN for Technical Support. COBAN is not responsible for lost data or information in the event of errors or other malfunction of the Software or computers on which the Software is used.

(f) Customer will have dedicated resources available to work 24X7 on Severity One and Severity Two Errors.

2.6 Maximum Number of Occurrences

(a) COBAN Limits the number of times a month a Severity One or Severity Two may be reported per customer to 10 occurrences per month combined and a total of 75 occurrences per year combined. Any additional occurrences after the 10th occurrence a month or 75th occurrence a year, whichever comes first, will be charged at COBAN's standard per incident rate. Refer to COBAN pricing sheet for per incident pricing at https://www.COBANTECH.com/support/pricing.html

3. Services Offerings and Fees.

3.1 Services Fee Terms.

(a) Services Fees are payable on the Effective Date or, in the case of a renewal term, no later than the date of commencement of the applicable Services Period. Services Fees are specified in the applicable price list and are non-refundable.

(b) In the event that Customer renews or adds a Services offering that has a minimum term of one (1) year, Customer may elect to make Services for all of its Software Licenses coterminous with the renewed or added Services. In such case, COBAN will prorate the applicable Services Fees to extend the current Services Period to make it coterminous with such renewed or added Services.

(c) For Software that is licensed on a perpetual basis, if a Customer purchases Services after acquiring the Software Licenses, or had elected not to renew Services and later wishes to re-enroll in the Services, Customer must move to the then-current Major Release of the Software and must pay: (i) the applicable Services Fees for the current Services Period; (ii) the amount of Services Fees that would have been paid for the period of time that Customer had not enrolled in the Services, and (iii) a twenty-percent (20%) reinstatement fee on the sum of the Services Fees in (i) and (ii).

(d) In cases where Customer purchases a License to migrate up from one edition of the Software to another (e.g., COBAN DVMS Standard to COBAN DVMS Enterprise), any unused period of the Services Period on the original License will be converted and used to extend the Services Period for the newly purchased upgraded License. This paragraph (d) shall not apply to enterprise license agreements.

3.2 Advanced and Complimentary Offerings.

(a) Certain Services (e.g., COBAN Mission Critical Support) require that Customer also purchase a base level of support. See the applicable price list for details.

(b) COBAN may offer complimentary Services, including COBAN Complimentary Update Services for certain Software, as more fully described at the COBAN Technical Support Services website. "**COBAN Complimentary Update Services**" means the provision of Maintenance Releases and Minor Releases, if any, to Customer. This COBAN Complimentary Update Service does not include the provision of any Major Releases.

(c) Services for Software made available under open source licenses may be subject to additional policies located at https://www.COBANTECH.com/support/policies/opensource.html

4. Miscellaneous Terms

4.1 Payment Terms. COBAN will invoice Customer for Services promptly following Customer's purchase. All invoices issued hereunder by COBAN are due and payable within thirty (30) days of the date of the invoice. By placing an order for Services, Customer represents that Customer is authorized pursuant to applicable laws and regulations to commit to payment prior to completion of the Services Period, as set forth herein. Services Fees are exclusive of any taxes, duties, or similar charges imposed by any government. Customer shall pay or reimburse COBAN for all federal, state, dominion, provincial, or local sales, use, personal property, excise, value added, withholding or other taxes, fees, or duties relating to the transactions contemplated by this Agreement (other than taxes on the net income of COBAN). Amounts not paid on time are subject to a late charge equal to the lesser of one and one-half percent (1.5%) per month or the maximum amount allowed by applicable law. If payment of any Services Fee is overdue, COBAN may also suspend performance until such delinquency is corrected.

4.2 Limited Warranty. COBAN warrants that the Services to be performed hereunder will be done in a workmanlike manner and shall conform to industry standards. Upon Customer providing COBAN with a reasonably detailed written notice to cure within thirty (30) days of occurrence of the nonconformance, COBAN will re-perform the Services to achieve commercially reasonable conformance with the above warranty. TO THE MAXIMUM EXTENT PERMITTED BY LAW, THIS WARRANTY IS GIVEN EXPRESSLY AND IN PLACE OF ALL OTHER WARRANTIES, STATUTORY, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. TO THE MAXIMUM EXTENT

MANDATED BY LAW, THIS REMEDY WILL BE CUSTOMER'S SOLE AND EXCLUSIVE REMEDY WITH RESPECT TO NONCONFORMANCE OF SERVICES.

4.3 Limitation of Liability. TO THE MAXIMUM EXTENT MANDATED BY LAW, COBAN SHALL NOT BE LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, WHETHER BASED UPON CONTRACT, TORT OR ANY OTHER LEGAL THEORY, ARISING FROM ITS PERFORMANCE OR NON-PERFORMANCE UNDER THIS AGREEMENT. BECAUSE SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE PRECEDING LIMITATION MAY NOT APPLY TO CUSTOMER. COBAN'S LIABILITY UNDER THIS AGREEMENT WILL NOT, IN ANY EVENT, EXCEED THE SERVICES FEES PAID BY CUSTOMER TO COBAN UNDER THIS AGREEMENT DURING THE TWELVE (12) MONTHS IMMEDIATELY PRECEDING THE DATE OF THE EVENT MOST DIRECTLY GIVING RISE TO THE CLAIM.

4.4 Termination. COBAN may terminate the Agreement and all Services at any time if (1) it is discovered that Customer is currently in breach of its Software license restrictions, pursuant to Customer's Software license or (2) Customer is in material breach of this Agreement.

4.5 Data Protection. Customer acknowledges that correspondence and log files generated in conjunction with a request for Services may contain sensitive, confidential or personal information. Customer is solely responsible for taking the steps it considers necessary to protect such data, including obscuring the logs or otherwise guarding such information prior to sending it to COBAN.

4.6 Other. Customer may not assign or delegate this Agreement to any third party without the prior written consent of COBAN. This Agreement shall be governed by the laws of the State of California without regard to conflict of laws principles. The parties consent to the exclusive jurisdiction of the state and federal courts located in Santa Clara County, California. This Agreement constitutes the entire agreement of the parties with respect to the provision of the Services by COBAN to Customer, and supersedes all prior written or oral communications, understandings and agreements. This Agreement may not be amended except in a written document signed by both parties. Any waiver of the provisions of this Agreement must be in writing to be effective. Except as expressly set forth herein, no terms of any purchase order or other business form that Customer may use will affect the obligations of the parties under this Agreement, and any such purchase order or other business form of Customer which contains additional or conflicting terms are hereby rejected by COBAN. Customer agrees that purchase orders do not have to be signed to be valid and enforceable. If any provision of this Agreement is found to be invalid or unenforceable, the remaining terms will continue to be valid and enforceable to the fullest extent permitted by law. The version of the Technical Support guide found at https://www.COBANTECH.com/files/pdf/support/tech_support_guide.pdf and the policies located at https://www.COBANTECH.com/support/policies/index/ are the governing versions of such documents/policies; any translation into other languages is for convenience only. COBAN may update the Technical Support guide and support policies periodically, without prior notice.