

RFP16000145 Data Breach and Credit Monitoring Services

Question	RFP Section	RFP Page	Question	Response
1	B7.3	31	What audits do you consider to be equivalent to a SOC2?	The State will not specify equivalent audits at this time. Offerors may propose alternative audits or standards that they believe “meet or exceed” the SOC2 audit. If you choose to propose an alternative, you must explain in detail in your proposal how the proposed alternate meets or exceeds the SOC2 standard.
2	B7.3	31	Do you consider a SOC1 Type II to be equivalent to a SOC2 audit?	No, SOC 1 reports are about controls at a service organization that relate to internal control over financial reporting. The State is concerned with quality of operational security controls, not financial controls.
3	B7.3	31	Are any of the following considered equivalent to SOC2: SSAE16 SOC1 Type II, ISO-27001 Gap Analysis, PCI-DSS, EU Safe Harbor, EI3PA?	The State will not specify equivalent audits at this time. Offerors may propose alternative audits or standards that they believe “meet or exceed” the SOC2 audit. If you choose to propose an alternative, you must explain in detail in your proposal how the proposed alternate meets or exceeds the SOC2 standard.
4	B7.3	31	What number of trust principles, and what specific trust principles are you requiring in regards to a SOC2 (security, availability, processing integrity, confidentiality, and privacy)?	All of the Trust Service Principles apply.
5	Exhibit C, Section b; Exhibit D, Section 2	37, 49	Section 10 of the Master Agreement Terms and Conditions (Exhibit C) provides a 15-day cure period, while Section 2 of the State of Idaho Standard Contract Terms and Conditions (Exhibit D) provides a 30 day cure period. Can these cure periods be amended to be consistent, with a 30-day cure period?	The State has considered the request and agrees to change the cure period to 30 days.

Question	RFP Section	RFP Page	Question	Response
6	Exhibit F	59, 60	Page 59 contains the pricing table for notifications and call center. Both of these are required to be price in Unit Prices. The scale starts at 0 and continues through 5 million. Page 60 contains the pricing table for one bureau credit monitoring/identity theft protection and three bureau credit monitoring/identity theft protection. Both of these also require Unit Prices, but the scale begins at 0 and tops out at 750,000. Why do the scales differ?	The pricing table for notifications and call center was developed based on an estimation of potential breach size. The pricing table for credit monitoring/identity theft protection was developed based on an estimation of how many affected individuals would sign up for the credit monitoring services in the event of a breach.
7	Exhibit F	60	On the pricing table for credit monitoring/identity theft protection, are your Number of Active Participants considered to be affected individuals who have actually redeemed a PIN code and successfully enrolled in an identity product?	Yes. Active Participants are Eligible Persons who have enrolled in the credit monitoring/identity theft protection services.