**Q&A for SDBOR IT Security Assessment**

1. Is there currently an incumbent company or previous incumbent, who completed a similar contract performing these services? If so - are they eligible to bid on this project and can you please provide the incumbent contract number, dollar value, and period of performance?

This is a new service request, and no incumbent service provider information exists.

1. Specify the VLAN details, how many are included in the scope?

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Question | SDSU | USD | BHSU | SDSMT | DSU | NSU | RIS | Total |
| How many vLans are in scope? | 5 | 20 | 2 | 6 | 8 | 6 | 21 | 68 |

1. Can you provide the current number of infrastructure details (physical servers, virtual servers, network devices, etc)?

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Question | SDSU | USD | BHSU | SDSMT | DSU | NSU | RIS | Total |
| How many physical servers? | 20 | 20 | 22 | 6 | 25 | 6 | 13 | 112 |
| How many virtual servers? | 300 | 220 | 130 | 10 | 250 | 67 | 300 | 1277 |
| How many external network devices? | 3 | 10 | 8 | 12 | 4 | 2 | 6 | 45 |

1. What is the percentage of the infrastructure in the cloud?

Little infrastructure exists in the cloud today aside from M365/Azure services. Less than 5%.

1. How many employees work in the IT departments?

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Question | SDSU | USD | BHSU | SDSMT | DSU | NSU | RIS | Total |
| Employees that work in IT department? | 60 | 60 | 15 | 15 | 20 | 20 | 23 | 213 |

1. Do you manage your own data center, or do you utilize any 3rd party/colocation facilities?

No 3rd party/colocation facilities are utilized outside of the SDBOR system.

1. What is the budget for this project?

The budget for this project will not be released at this time.

1. Clarification on the request for a “ransomware evaluation.” Is this a request for help identifying a vendor, or a request as part of assessing if the system has a problem with ransomware?

Assessing if the environment had a problem with ransomware, what would be the scope/impact. Also, highlighting heightened risks that may lead to a ransomware event.

1. Clarification on the “physical security assessment.” Is this related to the physical portion of IT systems (locations of servers, etc.), or is it a more true physical security assessment of the buildings (access points, cameras, lighting, etc.?

The physical security assessment is of less importance to the system but would include a walkthrough of on-site data centers for any glaring lapses or issues as it relates to security or resiliency.

1. Is there a plan to align all security policies, procedures, and documentation, considering they vary for all six universities and the board of regents? If yes, will that be part of the project?

There may be opportunities to review the standardization of security policies, procedures, and documentation within the Regental system, and any inclusion of those opportunities within the findings would be good to incorporate into the reports.

1. How many externally facing applications will be in scope?

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Question | SDSU | USD | BHSU | SDSMT | DSU | NSU | RIS | Total |
| Externally facing applications? | 30 | 20 | 10 | 15 | 75 | 10 | 30 | 190 |

1. How many applications will be in scope overall?

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Question | SDSU | USD | BHSU | SDSMT | DSU | NSU | RIS | Total |
| How many applications in scope? | 50 | 30 | 10 | 30 | 75 | 10 | 120 | 325 |

1. Are mobile or thick-client applications involved, or will only web applications be in scope? If other application types are in scope, please outline the numbers for each.

Web applications primarily. However, enterprise applications, like VMWare Horizon View, will be utilized within the system and reviewed as part of the penetration testing. No application specific reviews will be required on these types of enterprise applications.

1. How many network architectures, configurations, and firewalls are in scope for review?

There are 7 entities with their own networks with various configurations and firewalls. These networks may include multiple locations and firewalls.

1. The access control mechanisms and user privilege management of how many systems or architectures will be in scope?

The entire system is built within one Active Directory Forest and PAM services are moving to 7 separate cloud hosted instances of Delinea’s Secret Server platform. Each institution has their own processes for dealing with IAM that will need to be reviewed.

1. Will the assessment of incident response and disaster recovery plans only include documentation and implementation review or is active testing also required?

We do not expect active testing to be incorporated into the review process.

1. Do the incident response and disaster recovery plans differ between the six universities and the board of regents?

Yes, they vary greatly today based on each institution’s requirements.

1. Will the assessment of third-party and vendor management practices only include documentation review, or should samples also be reviewed?

We would like to understand if our third-party/vendor management practices and risk assessment/procedures are appropriate or if improvements could be made. If that requires samples/examples, then those could be provided.

1. Will the third-party and vendor management practices differ between the six universities and the board of regents?

Generally, the practices should be standardized as vendor onboarding and contract procurement has been incorporated into a system-wide process. However, variations do exist.

1. Does the physical security assessment include social engineering to get into specific rooms or access certain information? If yes, how many scenarios should be considered?

No, this is not necessary for our assessment.

1. Will the physical security assessment be conducted at all six universities and the board of regents? Are there any additional locations in scope?

While data centers may exist off campuses, we would primarily be interested in assessing only the ones that are on campus or easily accessible for review. This would be the 6 universities and the BOR data centers in Sioux Falls/Pierre.

1. Do the current security awareness training materials and programs vary between the six universities?

Each university and the BOR office select their specified materials/content and distributes it to their employees/participants via KnowBe4.

1. Will the risk assessment and risk management practices vary between the six universities?

Yes, there is no standardization today aside from a supplemental State-run risk assessment that is currently ongoing.

1. Do you want to conduct a complete NIST maturity assessment? If yes, we assume it needs to be executed six times (once for each university). Is this correct?

NIST has been the standard used by the BOR for previous internal assessments. However, USD has incorporated a CIS maturity assessment model and would prefer to build off their current program today if possible. We have conducted 7 assessments in our internal reviews previously.

1. Will the compliance requirements associated with GLBA, HIPAA, and FERPA be assessed for all six universities and the board of regents, or are there differences between the regulatory requirements for the universities?

The regulatory requirements would be the same across all seven entities; however, how those compliance requirements are being met, tracked, and reviewed will vary and we would like to understand any gaps in compliance. Some campuses may have more of a HIPAA requirement than others.

1. Will the ransomware-specific risk assessment be conducted individually against all six universities and the board of regents?

We would like 7 separate security assessment reports, including a ransomware-specific risk assessment incorporated. Risks should be mapped to ransomware.

1. Does the ransomware-specific risk assessment also include social engineering, or should we focus on the technical details and mitigating controls only?

An option for social engineering tactics could be reviewed, but we would like to focus on technical details and mitigating controls. Only the technical details will be part of the scoring.

1. Are there any expectations regarding the a-la-carte options for additional services, or are hourly rates sufficient?

We know that each vendor will likely have various expertise and additional services to offer, and we would like to understand what those offerings are and how they are typically priced. There are no set expectations for this request.

1. Please specify additional assessment services that you may be interested in, if any.

Any specific assessment services we have prioritized would already be identified within the RFP. This was added as an opportunity for vendors to offer services they feel would be beneficial to our system.

1. When should the vendor start executing the services?

We would like to begin assessments in early 2024.

1. Do you have any requirements regarding the deadline for deliverables?

There are no hard deadlines in place, but our normal cadence for security assessments and compliance reviews would have this completed in the late first quarter or early second quarter 2024.

1. Apart from the physical assessment, are any other parts of the security assessment expected to be executed onsite?

There is a preference to conduct most of the assessment’s interviews and reviews onsite to appropriately allocate time and be efficient. However, remote sessions are also viable unless we need to expand outside of the IT department resources.

1. Does South Dakota Board of Regent’s (SDBOR) have any choices of Penetration Testing/Vulnerability scanning tools? Does the Agency possess licenses for these Testing tools? Can the chosen firm leverage these tools/licenses during the engagement?

The SDBOR system utilizes Nessus/Tenable vulnerability scanning along with DHS external scans and PCI ASV scans to external CDE systems. Universities may have supplemental testing tools in place, but nothing is standardized. There is not a preference for the tools utilized and there is no licensing available for leverage in this agreement.

1. Please clarify if this is a single award or multiple award contract?

Single award for services across the system.

1. Please confirm if we need to provide live resumes for the key personnel.

Understanding the abilities and credibility of those performing the assessment will be necessary for our scoring matrix.

1. Can this work be offshored outside of the US?

There are security controls in place that would require the work to be conducted within the US.

1. Please clarify if the license cost of pen test tools will be borne by the vendor or the SDBOR.

The SDBOR does not have any licensing in place for penetration testing. The vendor would be expected to account for those costs in their pricing model.

1. Please clarify if there is any specific format that needs to be followed in the response.

There is no specific format required but examples of reports would be encouraged for us to review. The deliverables are defined in our scoring matrix provided as a response to another question for your review.

1. If we are shortlisted for an interview and if our proposed personnel are not available at that time, can we propose alternate resources for the interview?

Yes

1. Please confirm the mode of submission.

Proposals should be submitted via email to chris.phillips@usd.edu

1. Has the State had this type of assessment performed in the past?

The BOR has conducted internal security assessments annually and various third-party assessments have been conducted over the years at select institutions. This will be the first third-party, system-wide assessment for the SDBOR.

1. Regarding External Network Vulnerability Assessment and Penetration Testing, is exploit testing included in the external | internal network vulnerability scans?

We have decided to score only on external penetration testing services for this RFP as that is the priority for the system currently. Exploitability of identified vulnerabilities will be a key deliverable we would expect to receive as part of the testing. Exploit testing will likely require review as part of the initial engagement process as production environments cannot be put into any risk.

1. Regarding Internal Network Vulnerability Assessment and Penetration Testing, approximately how many IPs or subnets are in scope?

We have decided to score only on external penetration testing services for this RFP as that is the priority for the system currently and internal penetration testing scoping would require significant effort.

However, here are current IP address counts for your review:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Question | SDSU | USD | BHSU | SDSMT | DSU | NSU | RIS | Total |
| Internal penetration testing, how many IPs in scope? | 65000 | 65000 | 13,000 | 29072 | 65000 | 25000 | 5000 | 267072 |

1. Regarding Internal Network Vulnerability Assessment and Penetration Testing, can all internal network testing be done from a single location?

We have decided to score only on external penetration testing services for this RFP as that is the priority for the system currently and internal penetration testing scoping would require significant effort.

1. Excluding redundant or firewalls running in HA mode, how many firewalls are in scope?

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Question | SDSU | USD | BHSU | SDSMT | DSU | NSU | RIS | Total |
| How many firewalls? | 2 | 6 | 2 | 2 | 4 | 1 | 3 | 20 |

1. Is a Router | Switch Configuration Review in scope?

This was not anticipated to be part of the review.

1. How many routers | switches are in scope for a configuration review?

This was not anticipated to be part of the review.

1. Is the SDBOR open to sample-based testing?

It is important that a full review of each institution is conducted; however, sample-based testing of various services within each institution may be evaluated. IE... applications, systems, services, etc...

1. Is web application testing in scope?

We are not looking for a full web application assessment but would expect any publicly exposed web applications to be reviewed for vulnerabilities and insecure configurations/development practices.

1. How many web applications are in scope?

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Question | SDSU | USD | BHSU |  | SDSMT | DSU | NSU | RIS | Total |
| How many web applications in scope? | 30 | 15 | 8 |  | 25 | 50 | 10 | 120 | 258 |

1. Are the web applications Internet-facing or internal only?

We are primarily concerned with internet-facing applications and there are counts provided for each in previous questions.

1. Is enterprise application testing in scope?

Enterprise applications exposed externally would be in scope for vulnerability reviews and penetration testing.

1. How many enterprise applications are in scope?

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Question | SDSU | USD | BHSU | SDSMT | DSU | NSU | RIS | Total |
| How many enterprise applications in scope? | 30 | 15 | 0 | 2 | 25 | 0 | 1 | 73 |

1. Are the enterprise applications COTS or internally developed?

Enterprise applications are COTS. There are some internally developed solutions in use, but they are not used at an enterprise level.

1. Is a Database Security review in scope?

Yes, we would expect database configurations and security reviews to be part of the assessment process.

1. How many unique databases are in scope for database-specific testing for each institution?

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Question | SDSU | USD | BHSU | SDSMT | DSU | NSU | RIS | Total |
| How many unique databases are in scope for database-specific testing? | 20 | 20 | 3 | 0 | 0 | 0 | 10 | 53 |

1. If databases are in different locations, can all locations be reached from one central location?

No, they will be in several locations with access limited to internal institutional networks.

1. Is a Server Configuration Analysis in scope?

We would consider a review of the configuration baselines to be in scope but would not expect every server to be reviewed.

1. How many unique server brands are in scope for testing for each institution?

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Question | SDSU | USD | BHSU | SDSMT | DSU | NSU | RIS |
| How many unique server brands are in scope for testing? | 3 | 3 | 3 | 5 | 3 | 3 | 3 |

1. What devices does the Security Configuration Review cover?

We would not expect all network devices, servers, and workstations to be reviewed. However, we would like to incorporate into the assessment reviews of any existing hardening standards, their implementation, and overall network configurations as it relates to security.

1. Is a Wireless Network penetration test in scope?

No wireless penetration testing is required.

1. Is the wireless network controller-based or access-point-based?

No wireless penetration testing is required.

1. How many locations are in scope for wireless network testing?

No wireless penetration testing is required.

1. How many endpoints and workstations are in scope for each institution?

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Question | SDSU | USD | BHSU | SDSMT | DSU | NSU | RIS | Total |
| How many total endpoints? | 5000 | 5500 | 3,750 | 4100 | 5000 | 3500 | 375 | 27225 |
| How many workstations? | 4700 | 3200 | 1700 | 3500 | 1200 | 1200 | 75 | 15575 |

1. For physical security assessment, how many sites are in scope, and approximately how far apart are the sites?

There are 7 sites in scope with an average of 100 miles between sites.

1. Are there documented IT policies, procedures, standards, and guidelines in place, and are they aligned with a framework, such as a NIST CSF? If so, how many?

The BOR has a smaller set of policies that are enforced across the system. Each university additionally has a set of policies, procedures, and guidelines in place. The standard and count of each set of polices will vary for the 7 entities but it has been identified as a risk previously that our information security program, specific to these documents, has been lacking.

1. How many controls are included in the scope of the assessment?

We would expect typical controls to be reviewed within the scope including policies, procedures, measures, practices, and organization structures along with technical controls (firewalls, encryption) and procedural controls (staff training, response plans, etc..).

1. Is the disaster recovery plan comprehensive, formal, and documented?

Each institution manages their DR plan separately. The comprehensiveness of each version will vary.

1. Is the incident response plan formal and documented?

Each institution manages their IR plan separately but should incorporate aspects of the BOR’s system wide IR plan for consistency. The comprehensiveness of each version will vary.

1. How many data centers are in scope for testing?

We are primarily focused on the 7 main datacenters on each campus.

1. Is SDBOR currently using any service providers that are assisting in performing the requested services? If so, who are these providers?

No

1. What are the total number of assets to be factored for External Penetration testing?

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Question | SDSU | USD | BHSU | SDSMT | DSU | NSU | RIS | Total |
| How many servers are in scope for EXTERNAL pen test? | 50 | 80 | 10 | 30 | 70 | 9 | 150 | 399 |
| How many network devices are in scope for EXTERNAL pen test? | 3 | 12 | 2 | 12 | 4 | 2 | 6  | 35 |
| How many security devices are in scope for EXTERNAL pen test? | 1 | 6 | 2 | 3 | 75 | 2 | 6 | 95 |
| How many applications are in scope for EXTERNAL pen test? | 30 | 15 | 7 | 25 | 75 | 10 | 30 | 192 |
| How many external IP addresses are in scope for EXTERNAL pen test? | 150 | 400 | 14 | 123 | 50 | 9 | 30 | 776 |
| How many URLs are in scope for EXTERNAL pen test? | 150 | 50 | 8 | 23 | 15 | 30 | 30 | 306 |
| How many APIs are in scope for EXTERNAL pen test? | 0 | 0 | 0 | 0 | 0 | 10 | 0 | 10 |

1. What type of testing is desired as part of the External Infrastructure and Application Penetration testing scope? (e.g., BlackBox testing, Gray Box testing, or both).

Both would be desired as the system would like to fully understand our external exposure and providing information for a gray box test may prove insightful to provide more in-depth findings.

1. Can SDBOR share the frequency of External Penetration testing scope (e.g., Once, Monthly, Quarterly, Bi-annually, Annually).

DHS provides monthly external scans today. Today, no true penetration testing is being performed on regular occurrences.

1. How many network and systems are to be factored for Internal Penetration Testing scope? (e.g., servers, workstations, databases, and other internal resources).

We have decided to score only on external penetration testing services for this RFP as that is the priority for the system currently and internal penetration testing scoping would require significant effort.

1. Can the internal network Penetration testing be conducted remotely from a non-US based location?

We have decided to score only on external penetration testing services for this RFP as that is the priority for the system currently and internal penetration testing scoping would require significant effort. However, we would expect all services to be conducted within the US.

1. Can SDBOR share the frequency for internal Network Penetration testing scope? (e.g., Once, Monthly, Quarterly, Bi-annually, Annually).

No internal penetration testing is being conducted currently.

1. Are there any blackout periods or restrictions on testing times?

Yes, penetration testing will be subject to blackout periods that will need to be established as part of the initial project management meetings.

1. Does the Physical Penetration testing activities need to include Wireless Penetration testing? If yes, How many access points (APs) should be factored for the Wireless Penetration testing scope?

No wireless penetration testing is required.

1. Please specify the number of each application based on size:
Small - up to 50 web pages/ 25K LOC
Medium- up to 100 web pages/ 50K LOC
Large- up to 150 web pages/ 100K LOC
Extra Large - up to 200 web pages/ 150K LOC

Nearly all applications in scope would fall within the “small” category for web pages and would have limited lines of code, especially those that are custom developed.

1. Are any of the in-scope applications only exposed internally?

We are focused on internet facing applications.

1. Do Private/Public/Open APIs involve multiple endpoints, data formats, or custom protocols? If yes, please share further details about these endpoints, data formats, or custom protocols.

There is little to no use of Private/Public/Open APIs that are hosted from our environments today.

1. What are the approximate number of rule sets configured in each of these firewalls? Please, specify the number of firewalls separately.

While not broken down by each firewall, here is an average of firewall rules per firewall to give you an idea for sizing.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Question | SDSU | USD | BHSU | SDSMT | DSU | NSU | RIS | Total |
| How many rule sets are configured on average per firewall? | 1500+ | 1500 | 250 | 98 | 100 | 100 | 200 | 2248 |

1. For configurations, rules sets, ACL, policies and segregation review of the in-scope firewalls, will SDBOR provide the testers with a dump of the firewall rules, configuration, network diagrams, documents and required details of the different environments? (e.g., development, testing, production).

We are willing to provide a running configuration of the information referenced for review.

1. Please specify the number of rounds of validation testing that needs to be factored in as part of the entire assessment scope (e.g., a single-time testing with one-time revalidation?

This would be a single-time test for the system to understand current exposure/risks.

1. Can you share details on what is in-scope for the network architecture review?

Network diagrams will be provided for your review and evaluations of risk as it relates to network resiliency, datacenters, and cloud connections would be ideal.

1. How many privileged users are in-scope for this particular assessment?

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Question | SDSU | USD | BHSU | SDSMT | DSU | NSU | RIS | Total |
| How many privileged users are in-scope? | 103 | 100 | 6 | 10 | 20 | 10 | 25 | 274 |

1. Are Security Architecture diagrams available for the in-scope applications?

Security architecture diagrams would likely not be available/developed for review.

1. Is SDBOR leveraging a GRC tool? (E.g. Archer, ServiceNow, KeyLight etc.)

No GRC tools are in place today.

1. What is the preferred duration of the assessment?

The overall duration of the assessment for the system is less of a concern as compared to the duration/time investment required for each institution and the time to expected deliverables. Ideally, the full assessment with deliverables in hand would be completed by July 1st.

1. Can we provide an A La Carte option based on blended hourly rates?

Yes

1. Can SDBOR confirm if the vendor needs to provide cost for each entity separately?

Initial pricing does not need to be broken down by an institution. However, we may request such a breakdown upon contracting services.

1. Will there be a main point of contact at each institution to coordinate the work with?

Yes

1. Will there be an executive point person assigned to the project?

Yes

1. Pre-assessment planning: How many policies and procedures will need to be reviewed per institution?

This will vary by institution with USD/SDSU having around 15 in place and the rest having less to review.

1. Pre-assessment planning: Is this an in-person or virtual meeting? Is this a collective meeting with all institutions or individually?

This could be conducted virtually and if kept high-level, could be utilized to baseline expectations/requirements across the BOR. Anything involving technical review would require separate meetings by institution.

1. What is the firewall make, model, and quantity at each institution?

The system has standardized on Cisco firewalls with most running 3130’s.

1. Can you clarify the proposal response deadline?

Proposals are due on 12/7/2023 and should be submitted via email to chris.phillips@usd.edu

1. For in-scope applications: How many applications are there to be tested?

Already answered previously, but we are not looking for full application specific assessments to be conducted. We are rather looking for vulnerability testing to be conducted on external facing applications and any exploitability. There will be a few applications that are custom developed and some that will be COTS. However, we do not feel that providing functionality, sizing, type, users, or form counts will provide any valuable insight for your proposals based on our clarifications of how we would like application reviews conducted.

1. For in-scope applications: What is the primary function of each?

Already answered previously, but we are not looking for full application specific assessments to be conducted. We are rather looking for vulnerability testing to be conducted on external facing applications and any exploitability. There will be a few applications that are custom developed and some that will be COTS. However, we do not feel that providing functionality, sizing, type, users, or form counts will provide any valuable insight for your proposals based on our clarifications of how we would like application reviews conducted.

1. For in-scope applications: What is the type of each (web/mobile/Windows)?

Already answered previously, but we are not looking for full application specific assessments to be conducted. We are rather looking for vulnerability testing to be conducted on external facing applications and any exploitability. There will be a few applications that are custom developed and some that will be COTS. However, we do not feel that providing functionality, sizing, type, users, or form counts will provide any valuable insight for your proposals based on our clarifications of how we would like application reviews conducted.

1. For in-scope applications: What is the size of the application?

Already answered previously, but we are not looking for full application specific assessments to be conducted. We are rather looking for vulnerability testing to be conducted on external facing applications and any exploitability. There will be a few applications that are custom developed and some that will be COTS. However, we do not feel that providing functionality, sizing, type, users, or form counts will provide any valuable insight for your proposals based on our clarifications of how we would like application reviews conducted.

1. For in-scope applications: What are the number of users per?

Already answered previously, but we are not looking for full application specific assessments to be conducted. We are rather looking for vulnerability testing to be conducted on external facing applications and any exploitability. There will be a few applications that are custom developed and some that will be COTS. However, we do not feel that providing functionality, sizing, type, users, or form counts will provide any valuable insight for your proposals based on our clarifications of how we would like application reviews conducted.

1. For in-scope applications: What are the number of forms per?

Already answered previously, but we are not looking for full application specific assessments to be conducted. We are rather looking for vulnerability testing to be conducted on external facing applications and any exploitability. There will be a few applications that are custom developed and some that will be COTS. However, we do not feel that providing functionality, sizing, type, users, or form counts will provide any valuable insight for your proposals based on our clarifications of how we would like application reviews conducted.

1. Are there additional details as to how the evaluation criteria will be weighed?

There are not any additional details as to how the evaluation will be weighed.

1. How many students does each University have?

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Question | SDSU | USD | BHSU | SDSMT | DSU | NSU | RIS | Total |
| How many students? | 11327 | 10,000 | 3475 | 2893 | 2917 | 2932 | 0 | 33544 |

1. How many faculty and administrators does each University have?

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Question | SDSU | USD | BHSU | SDSMT | DSU | NSU | RIS | Total |
| How many faculty/admins? | 2556 | 2250 | 383 | 460 | 436 | 379 | 0 | 6464 |

1. How many users are in each in-scope institution?

Everything is in scope for the security assessment. If this is for social engineering scoping, we would expect that to be out of scope.

1. What is the approximate number of Windows servers?

Windows servers make up roughly 90% of our total server counts.

1. Please list any other operating systems and how many.

MacOS makes up 10% of workstations and Linux makes up around 22% of servers.

1. What is the approximate number of switches?

There are a significant number of switches in use today. Based on previous answers regarding configuration reviews, it is assumed that the exact number of switches is no longer pertinent to scoping.

1. For IDS/IPS (intrusion detection) – does each site utilize one and if so is it locally managed?

Yes, and Yes

1. Are there any persistent connections to 3rd party vendors (HVAC, IT service provider, etc) that are in-scope?

No

1. Do you use any cloud environments such as Azure or Amazon Web Services that are in-scope?  Do you know which vendors?

The system utilizes Azure cloud environments we would like included in the security assessment review process.

1. Are there any remote access services in scope (on-demand VPN, GoTo my PC, LogMeIn, etc.)?

On-demand VPN, VDI

1. How many employees have remote access?

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Question | SDSU | USD | BHSU | SDSMT | DSU | NSU | RIS |
| How many employees with remote access? | 200 | All | 50 | All | 20 VPN | 150 | 50 |

1. Are there any in-bound modems in use?

None in scope

1. For the security assessment, do you want production tested, or a non-production location?

Due to lack of non-production environments, production will need to be evaluated in most cases.

1. How many WAFs are included in the security assessment?

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Question | SDSU | USD | BHSU | SDSMT | DSU | NSU | RIS | Total |
| How many WAFs in use? | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 2 |

1. Where are the locations in-scope for the physical site visits?

Pierre, Vermillion, Brookings, Rapid City, Spearfish, Madison, and Aberdeen South Dakota

1. Are the in-scope location physical assessments for penetration for overall review/assessment?

We are not expecting the physical assessment to include penetration reviews. The physical assessments are not as high of a priority and would only include the data centers that are reasonable to evaluate based on distance/time restrictions.

1. Will you accept a separate redacted proposal to be used in the event a public records request is made?

Only the awarded vendor’s proposal would be subject to a public record review. If there is a request to review the winning proposal the awarded vendor will have an opportunity to provide redactions at that time.

1. RFP Sections 6.1.4 and 6.1.5 list “Availability to the project locale” and “Familiarity with the project locale” as evaluation criteria. Can SDBOR please define “project locale”?

The State of South Dakota would be the project locale.

1. RFP Section 3.0 Scope of Work, specifically section 3.2.1.3.1 states “Compliance Frameworks: GLBA, HIPAA, Cyber Insurance”, the NIST CSF is mentioned in section 1.1 and other areas. Is NIST CSF one of the frameworks in scope?

We have used the NIST framework for previous internal assessments conducted by the BOR on our institutions. There would be a desire to utilize this framework within the vendor's assessment to correlate findings to previous findings.

1. Is the comprehensive report intended to be one overall report or one report per institution?

We would like a comprehensive report for each institution for their leadership to review/analyze along with a system wide report for BOR reference.

1. Will the scope of the assessment be the same for all Universities?

Yes

1. Does SDBOR have a preference for contracting a local firm for this work? If so, what weight will this have in the evaluation process?

The criteria to be used in the evaluation is listed in Section 6.0 of the RFP. This is the only criteria that will be considered.

1. Has SDBOR worked with an external consultant for any earlier efforts related to information security? If yes, who and what was the nature of the project(s)?

There have been no previous information security projects outsourced to vendors/consultants that correlate to this project.

1. Does each institution have their own IT/IS policies and procedures?

Yes

1. To what extent do institutions rely on BOR/RIS services and policies/procedures?

The BOR manages central applications that are utilized across the system. BOR policies do roll down to each institution, but a significant percentage of the information security policies are currently managed at a university level.

1. Do all institutions and the BOR have cybersecurity insurance? If so, is it the same coverage and are requirements the same?

We are all under one umbrella and requirements for cyber liability insurance.

1. Can we run services and various parts of the assessment simultaneously? For example, Pen testing and IT security assessment going on at the same time?

Yes

1. For 3.2.2 (Review of network architecture, configuration, and firewall rules,) – Is this work to be completed at each institution and the System Office, or just the System Office?

6 universities and BOR office.

1. 3.2.7 (Review of security awareness training materials and programs) – Are we reviewing the security awareness training materials to confirm they exist or are we evaluating the materials to see if the content is relevant and includes updated best practices?

We know the security awareness programs are implemented across the system as we have a central KnowBe4 instance. This item would include reviewing completion of those programs by institutions and providing recommendations for any gaps in specific role-based training needs.

1. Is the training system wide or per each institution and system separately?

We are standardized on KnowBe4, but each institution manages their training separately.

1. 3.2.8 – Are we reviewing the categories under 3.2.8.1 to ensure they exist at each institution and the System Office or are we conducting a GLBA assessment along with the IT Security Assessment?

Either would be acceptable and the service options could be broken down within your proposal. The goal is to ensure that GLBA compliance is being met by all 7 entities within the system.

1. Is this one GLBA process per the system or for each institution and the system?

GLBA compliance is required for all 7 entities to achieve, so it would be each institution.

1. 3.2.10 - Normally in our IT Security Assessments we provide feedback on any finding/vulnerability we discover for various compliance regulations, is this an acceptable approach in the assessment or the desire for additional time to be earmarked to review such compliance regulations to report discovered finding/vulnerabilities as listed in this section?

Incorporating it into the full assessment is acceptable.

1. 3.2.11 – Is this an assessment to be performed at each institution or at the system? Is the process to address a ransomware event the same for each campus?

We would expect 7 separate security assessments (6 universities and BOR). Ransomware does not need to be a separate assessment/report, but we want to understand where specific risks that could lead to a ransomware event exist today.

1. 3.3.2 – “and plan to incorporate the security assessment findings and mitigation recommendations.” Is this part of the overall report or a separate report?

It can be presented as the vendor sees fit, provided we receive both the identification and suggested remediation/mitigation tasks.

1. In the case where, on a single campus, there are multiple buildings that house data center facilities, does each building need to be evaluated, or should all buildings be considered managed and secured in the same way? Which campuses have multiple buildings with data center facilities?

It should be noted that we are less concerned about physical security assessments; however, a walk-through of the main data center on campus for any glaring issues with security would be beneficial. Multiple buildings will not need to be reviewed.

1. 3.2.8.1 - For the items listed as elements that should be included in the assessment, are you referring to the existing assessment that you want examined in line 3.2.8? Or are these elements that you are looking to have included in the assessment for which we are submitting a proposal?

Per GLBA requirements, we are looking to include the elements in 3.2.8.1 within the risk assessment identified in 3.2.8. These elements are identified within the GLBA Safeguards Rule to which we are verifying compliance. A version of this risk assessment should exist at each campus today, as the rules are already in place. This request is to verify compliance is being met and the risk assessment is comprehensive.

1. 3.2.10 - Can you elaborate specifically around the FERPA requirements, and the assessment details you are looking for?

We would anticipate the vendor would be familiar with FERPA compliance requirements and would be able to specifically call out any concerns and/or gaps when performing the overall security assessment. However, if the vendor provided a specific FERPA review, we would look at it as an a-la-cart or add-on option to services.