STATE OF SOUTH DAKOTA
OFFICE OF PROCUREMENT MANAGEMENT
523 EAST CAPITOL AVENUE
PIERRE, SOUTH DAKOTA 57501-3182

Cyber Security and Privacy Assessment Services

PROPOSALS ARE DUE NO LATER THAN MAY 31st, 2022 5:00PM CDT

RFP 2767 **BUYER**: Department of Social Services, Operations office **POC**: Dawson Lewis Dawson.Lewis@state.sd.us

General/RFP Clarifications

* Are delivery timeframes flexible?
The initial timeframes for 2022 are not.
* Which Agencies will be in-scope (RFP Section 3.1.2, 3.1.3)
Department of Social Services. The Division of Medical Services, Division of Child Support and Division of Economic Assistance. In addition, please outline your methodology for reviewing other divisions within Social Services to determine if they should be included based on their processing of federal funds. Upon initial review, other divisions may be determined to be included to complete this review. Those identified will be incorporated into subsequent reviews.
* Are we assessing the system alone, or all departments' policies as well? (RFP Section 3.3 ADP, 3.5 MARS-E)
Both
* Do you want us to test your certification as a part of this engagement? (RFP Section 3.1.7)
For the initial review, no. However, we may add this on to subsequent years.
* 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?
Yes. They are eligible to bid and have been doing parts of this for 15 years. That said this is a true RFP whose purpose is to look at new firms to see if there are better ways to perform these reviews

* What is the approximate budget?
We decline to answer
* Do you maintain vulnerability management procedures that include identifying and remediating technical vulnerabilities?
We have been doing that with our current vendor. We expect that part of your solution will be to provide us either with tools or recommendations for tools to do this.
* Does your organization have an integrated SOC with SIEM solution (i.e., ArcSight, Splunk, etc.) to aggregate and assess threats and respond?
No
* In RFP page#2 under section 1.1 it is indicated that "Therefore, we are looking for an offeror or offerors who can work with the DSS and BIT to analyze and test our various systems to make sure that we are in compliance with various Federal regulations" **Question**: What federal regulations and security compliance are followed by DSS?
Please refer to section 3.1.3 of the RFP
* Does DSS have multiple cybersecurity compliance frameworks associated with their organization?
Please refer to Section 3.1.3. There are overlapping regulations and different offices may need to comply with different guidelines. For example, both IRS and CMS are under the NIST framework but have variations in their respective guidelines.
* Is there any pending vulnerability assessment that is currently in line with DSS? If yes when it will be completed?
No, nothing is pending
* When was the last security assessment completed for your organization? Are all the vulnerabilities mitigated already?
In 2021. No, they not all been mitigated.
* What are the critical business systems that are used in day-to-day operations in DSS and their subdivision? Please provide the total number of systems

There are approximately 50 systems which may be included in the scope of your proposal. These would include systems for Child Support payments, Economic Assistance and others. A complete list of application would be provided to a successful bidder.

Questions about network size / scope

* Specify the VLAN details how many are included in the Scope?
This information will not be disclosed without an agreement in place to protect confidentiality.
* Approximately how many computer endpoints do you have (desktop PCs, laptops, servers)?
1,100
* What's your headcount of users (employees + contractors+interns)? What number/percentage of your workforce resides within organizational facilities? What number/percentage works remotely?
Approximately 500 employees work within divisions covered under this work. Most of them have the ability to work remotely but do not.
* How much (%) of the infrastructure is in the cloud?
We are in the process of moving to an internal cloud. It is not complete but we do not have a current percentage done.
* What is the size of the IT environment?
DSS has approximately 1100 computer users.
* How many physical locations?
The main locations are the Human Services Center in Yankton and the Kneip Building Pierre. We have 30 some satellite offices.
* What is the aggregate Internet Capacity per location (<300mbps, <1gbps, <4gbps, up to 10gbps)?
10gps
* Do you manage your own data Center, or do you utilize any 3rd-party/colocation facilities?

BIT manages the data center.

External Network Vulnerability Assessment / Penetration Testing

* Please select a testing approach from: black box (no knowledge) testing, gray box (some knowledge), or white box (complete knowledge)? Each has its benefits and time considerations and costs. (We would recommend the Gray Box approach for cost and efficiency benefits).
We would prefer Gray box. However, vendors can present other options with their associated Pros and Cons.
* Total number of public facing / external network IP addresses to be tested (If providing an IP range, please indicate the estimated number of live IPs). * Number of Web based applications/ services to test (dynamic pieces of websites that users or other application authenticate to – client portal, sales quote system). * How many web applications are in scope
We have five (5) public facing web applications
* Number of VPN, Terminal Services, Remote Desktop, FTP, and other remote services to be tested * Can you please provide the current number of infrastructure details (Physical Server, Virtual Server, Network Devices etc.
This information will not be disclosed without an agreement in place to protect confidentiality.
* Is an objective of this test to also assess the Company's intrusion detection capabilities?
Typically, yes. We have conducted tests in the past without notifying the full network security team in order to test their responsiveness.
* How deep should testing go in the event of successful network penetration (i.e. just validation of vulnerability; network administrator access; server access, etc.)?
We would want only the validation of the vulnerability. If vulnerabilities are discovered a vendor would immediately need to stop and contact DSS and BIT. It may be that we would have the vendor pursue the flaw but only under the supervision of BIT.
* Are the external systems hosted by a third-party provider?
There are some systems that are owned by third parties.

* Does your organization own and manage the network equipment at your external perimeter?
BIT manages State networking equipment.
* Has there been penetration testing performed in the last one year? If yes, can you please let us know the penetration testing was done for external environment only or internal network also?
Yes, in 2021. It was done for external networks.

Internal Network Vulnerability Assessment / Penetration Testing

* Total number of internal network IP addresses to be tested (If providing an IP range, please indicate the estimated number of live IPs).
We are undecided at this time as to doing this. Vendors are welcome to propose this as an option and discuss costs.
* How deep should testing go in the event of successful network penetration (i.e. just validation of vulnerability; network administrator access; server access, etc.)?
We would want only the validation of the vulnerability. If vulnerabilities are discovered a vendor would immediately need to stop and contact DSS and BIT. It may be that we would have the vendor pursue the flaw but only under the supervision of BIT.
* Are internal web-based applications / services in scope, if so, please provide an indication as to the anticipated number of web-based applications/services that may need to be assessed.
There are three identified at this time. In your proposal you should discuss what you see as the average time and effort needed to test applications.
* Is it desired to evaluate the strength of mobility environments (iPhones, BlackBerry, home VPN access)?
No, not at this time.

* Are corporate build / configuration standards in place for various platforms (network devices, operating systems, etc.) and if so, is it desirable to evaluate against those standards, etc. This will determine the amount of time required to perform additional analysis and tuning of evaluation criteria.
No, we would not like this in the current scope of work.
* Can remote internal networks be scanned via a primary location or would it be necessary to perform field visits to each in-scope location?
Field visits will not be needed.
* Are any of the internal application a third-party provider?
Yes

Wireless Security Assessment

* Will Wi-Fi testing be conducted at each location? If so, how many SSIDs and which locations?
This is out of scope for this project.
* Please provide an estimate of the types of Wireless in use (microwave, 802.11x, proprietary, cell phone, blackberry, iPhone, Bluetooth, Point-to-Point, etc.).
N/A
* Are formal wireless security policies in place?
N/A

Mobile

* What Mobile Platforms are in scope?
Mobile platforms are not in scope.
* How are Mobile devices being used for; e.g. email, two-way comms, application interfaces, GPS, mobile applications?
N/A

Facility Breach

* Number of Facilities in scope?
Facility breach testing is not in scope
* To what level should the unauthorized access be demonstrated? (access to paper files, office areas, network access, obtaining equipment, etc.)?
N/A

External War Dialing Exercise with Modem Penetration Test

* Please provide an estimate of the number of telephone numbers that are in scope.
This is not in scope
* Please provide an indication of acceptable dialing times or special requirements around when it is acceptable to dial phone numbers (e.g., are business hours off limits?).
N/A
* Is dictionary-based password guessing an acceptable procedure for identified modems and voice mail boxes?
N/A
* Please provide an estimate of the number of modems.
N/A

Firewall Rule Set Reviews

* Please provide the number of in scope firewalls to be reviewed.
This is not in scope
* Are there Company firewall policies / standards in place that the assessment will test against for compliance, in addition to best practices?
N/A

* Please provide firewall make and model for in-scope devices.
N/A

VoIP Security Assessment

* Please provide an indication as to the number of centralized management consoles for VoIP systems.
This is not in scope
* Please provide an indication as to the degree of separateness the VoIP network has from the data network or are they two converged?
N/A
* To what degree of security is the VoIP assessment desired? For example, if it can be shown that the testing team is capable of intercepting voice mails or eavesdropping on phone calls, would that be of value?
N/A
* Are soft VoIP phones in use?
N/A
* Is it desired to identify abuses of the VoIP system (fraudulent calls, excessive long distance, etc.)?
N/A
* Is voicemail box penetration testing an acceptable procedure?
N/A

DMZ Architecture Review

* Number of systems and devices in the DMZ architecture to be reviewed
This is not in the scope of this project

* Are updated network diagrams available?
N/A
* How recent is the DMZ architecture documentation (diagrams, etc.)
N/A
* Would it be necessary to verify physical connections in data centers or other locations, if so, please provide estimate of the number of physical locations to visit to identify potentially unauthorized physical links that may bypass firewall protections (e.g., dual homed hosts).
N/A

Remote Social Engineering

Types of Social Engineering approaches:
* Impersonation: If there is a person within the company you would like us to impersonate in order to gain access to information, please indicate who this should be. Otherwise, we will decide based on factors including tenure, position, and possible influence.
This is not in scope. It is handled by BIT
* Important User: We may make references to known associates or important users in order to influence someone's decision to provide us with information on their behalf. Please indicate who this 'important user' should be. Otherwise, we will decide based on factors including tenure, position, and possible influence.
N/A
* Third-party Authorization: We may make claims that permission has already been granted by another associate for information.
N/A
* SPAM: Do you wish for us to generate false advertisements in hopes of detecting users who decide to click on ads and hyperlinks?
N/A

* Spear Phishing: Through the process of sending an e-mail to users and falsely claiming to be a legitimate enterprise, we can potentially coerce a user into disclosing private information. Please indicate if this is a required assessment.
N/A
* Will USB drops be included as part of the exercise? If so, how many USB would you like to deploy and how many locations?
N/A
* Will Physical Facility Breach be included as part of the exercise? If so, how many locations will be in scope?
N/A
* Can employees log into webmail remotely? If so, what is the webmail URL?
N/A
* Is email hosted internally? If not, who hosts the email services?
N/A

Secure Code Reviews

* Please provide an indication as to the number of lines of code, the languages (e.g., C, C#, HTML, Web 2.0, ASP, etc.), the number of applications, etc. to help determine what is meant by “security code” review.
This is not in scope
* Are automatic source code evaluators acceptable (they are expensive!)?
N/A
* Are developers available for interview and confirmation of suspected problems?
N/A
* Would it be possible or desired to perform grey box testing in conjunction with external penetration testing and DMZ architecture review?
N/A

Cloud Services Administration Review

* What services are provided by a cloud provider (AWS, Google, Microsoft, etc.)
This is not in the scope of this RFP
* Do you manage your cloud services yourself? If so, which functions are performed in-house versus by the cloud provider?
N/A
* Do you have an architecture diagram of you cloud environment(s)? If yes, can you provide?
N/A

Cybersecurity Liability Insurance Review

* Do you currently carrier cyber liability coverage? If so, who is the carrier and what are the limits? Do you feel your policy adequately addresses your exposure and it's tailored to meet your specific needs?
This is not in scope
* Have you had any coverage related losses in the past 5 years?
N/A
* Do you wire funds in excess $25,000 other than for payroll or deposits to a financial institution?
N/A
* How many records with PII or PHI do you have, where are they stored and do you follow an active record retention program?
N/A

Digital Forensics

* Is criminal or civil litigation involved now, or expected in the future?
This is not in scope
* Provide a description of the objectives to achieve (file recovery, analysis of user behavior, etc.)
N/A
* Indicate any timelines, milestones, due dates, etc.
N/A
* Number and type of in-scope devices, with storage capacities? (two 32Gb iPhones, one laptop with 1Tb HDD, 128Mb SD card, etc.)
N/A