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

HIPAA Security Risk Audit

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

RFP 2766 **BUYER**: Department of Social Services, Office of the Secretary, Operations office **POC**: Dawson Lewis Dawson.Lewis@state.sd.us

Clarifying the RFP

* Our understanding is that you're seeking a vendor that can provide a comprehensive HIPAA Security Risk Assessment of both your electronic and physical security for information covered by HIPAA. However, the scope of work indicates a request for more of a HIPAA Compliance Audit – can you provide clarity on the required scope? Are you seeking a Security Risk Assessment, a HIPAA Compliance Audit, or both? * Is DSS looking for a Risk Assessment to satisfy 164.308 (a)(1)(i)(ii)(A) – Risk Analysis and 164.308 (a)(1)(i)(ii)(B) – Risk Management, or is the intent of the engagement to be an assessment of policy, procedures and controls in place to meet all of Part 164, Subpart C (Administrative, Technical, and Physical Safeguards)? * What are the expectations for audits? Will the requirements under this RFP be for an audit or security and compliance assessment? * Does this assessment include an independent risk analysis?
The vendor will need to perform an evaluation as described in 164.308(a)(8).
* Regarding section 3.2.3, is DSS anticipating any services beyond the HIPAA risk assessment to be performed, such as vulnerability scanning or penetration testing?
These are covered under RFP 2767 Cybersecurity Audit.
* As DSS is a Hybrid Entity, which part of the entity is under this audit? * What are your individual programs that are in-scope? (RFP Section 3.2.2)
For a list of entities see page 28 of the RFP under Hybrid Designation

∗ Does DSS anticipate remediation consulting between bi-annual assessments?
We would like this to be presented as an optional service. Include as an attachment labeled “Optional Bi-annual assessments” with its own cost proposal.
∗ What is the approximate budget? ∗ Does DSS have a budget they are willing to share with the potential vendors?
We choose not to share the budget
∗ 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.
∗ Page 5, 3.0 Scope of Work, Item 3. 2.2. Are you seeking how we might do things differently if you add individual programs to the project?
What we are looking for is your methodology how you would look at programs not already in scope to determine if they should or should not be added to a HIPAA review
∗ Page 5, 3.0 Scope of Work, Item 3.2.3. Are we to assume that this is the entire DSS agency IT infrastructure or a specific segment?
Similar to the above question, we are looking for your methodology of how you would assess our systems. The goal of 3.2.2 and 3.2.3 is to leverage vendor expertise to find areas we have overlooked. We are wanting to know ***how*** you would look for such “holes”
∗ Section 6 ‘Proposal Evaluation & Award Process’ lists the criteria in order of importance. Can you provide a detailed weighting of each line item?
The greatest weight will be given to 6.1.1 through 6.1.5
∗ Are delivery timeframes flexible? ∗ In regards to 3.6 “the initial audit report should be delivered by September 30, 2022” Does initial equate to Draft/first iteration of report for DSS comment prior to finalizing? If yes, does DSS have a final delivery date to target?

Initial in this case means the first completed report in what we hope will be a series of four reports over the coming 7 years.
* Do you allow sub-contracting?
Yes. They will be subject to the same policies on background checks and security guidelines that you as the main contractor are. You must clearly delineate how you propose to use subcontractors.
* Sections 3 and 4 do not mention the proposer's personnel. But 6.3 reads, "The qualifications of the personnel proposed by the offeror to perform the requirements of this RFP, whether from the offeror's organization or from a proposed subcontractor, will be subjectively evaluated. Therefore, the offeror should submit detailed information related to the experience and qualifications, including education and training, of proposed personnel." So the question is where in the proposal do you want to see information about our personnel? In the Detailed Response section?
We do not have a fixed standard for this. Typically, what we see is that vendors will mention key staff in their detailed response. Then towards the end of their proposal provide their resumes.

Physical

* Physical Street address for each location * How many physical locations need to be assessed? * How many locations/buildings are included for this assessment? * How many physical locations? * How many physical locations included in the in-scope environment to be assessed? * Estimated Square footage of the location * How large is each physical location that needs to be assessed? * Total Number of Employees * Average daily census (Avg # of PT at this location)
We will have physical reviews of security at the Human Services Center (HSC) in Yankton, South Dakota and at the Richard Kneip Building in Pierre, South Dakota. There are approximately 500 employees at HSC. Approximately 300 in the Kneip building. HSC – approximately XXXXXX in 15 buildings on campus Kneip – approximately 32,000 sq ft
* Our understanding is that you're looking for our response to our approach to on-site visits. Do you anticipate the vendor visiting all sites or conducting a sampling? If sampling, do you have a preferred percentage of sites to be sampled? *Section 3.2.4.3 states 'If planning on-site visits, what is your plan for our offices outside of Pierre. See Attachment D – Town and Cities with DSS Offices' –* Can you please provide the number of interviews that are expected for each office? * Page 5, 3.0 Scope of Work, Item 3 2.4, Physical Safeguards. Are you allowing in-person reviews for this element of the project? * What is the expectation for percentage of sites being checked? (RFP Attachment D)
Only the two sites mentioned above.
* Is there on-site storage of paper medical records or other PHI? * Does each facility have defined method for proper destruction of PHI?
Yes, to both
* Total Number of Providers
Not sure as to what this is asking. The assessment is limited to the DSS entities that are part of our Hybrid Designation and BIT as both a Business Associate and provider of our IT resources.

* Will the Organization provide an escort with appropriate access to all secure areas?
Yes

Administrative Safeguards

*Does the Organization have designated Privacy and Security Officials? *Have DSS assigned responsibility for implementing and maintaining the policy & procedures for HIPAA compliance and ePHI related data security? If yes, who is responsible?
Yes, our Legal Division
* Total number of policies * How many cybersecurity policies are in-place for the in-scope environment? * Are there any information security functions that exist already in DSS that work on RISK mitigation/treatment plans? * What is the approximate size (number of policies and/or page count) for the HIPAA Privacy and HIPAA Security manuals for both HSC and DSS?
Please refer to Attachment G BIT Information Technology Security Policy (ITSP) https://dss.sd.gov/docs/rfp/2766/RFP_2766_ATTACHMENT_G.pdf
* Average number of policies reviewed and edited annually. * How many cybersecurity policies are in-place for the in-scope environment?
Please see Attachment G BIT Information Technology Security Policy (ITSP) https://dss.sd.gov/docs/rfp/2766/RFP_2766_ATTACHMENT_G.pdf
* Do you have Risk Management procedures in place that require a Risk Assessment be completed to evaluate compliance with the HIPAA Security Rule?
To this point we have used our regular audits that comply with Federal regulations as our basis for evaluation. We do not have a separate state policy.
* Do you perform periodic technical and non-technical evaluations of the HIPAA standards under this rule and in response to environmental or operational changes affecting the security of ePHI?
BIT is our BA as it relates to DSS's databases, network, applications, email gateway, and our ePHI; and that they conduct technical assessments as IT changes are made.

* Who in the Organization manages policy approvals?
Our Legal Division
* May we request a sample of annual HIPAA Training?
We are currently onboarding a new provider so we do not have material to share at this time.
When was the most recent Security Risk Assessment conducted?
2017
Does the Organization have defined Business Continuity and Disaster Recovery Plans?
Yes
* Does the Organization have Incident Response procedures, are they tested, if true what frequency? * Do you have policy & procedures in place to respond to emergencies that damage systems containing ePHI?
Yes. However, we do not have regular tests
* Does the Organization have a defined process to manage Business Associate Agreements?
No
* Do all Business Associates use the DSS BAA template, or are there agreements using the Business Associate's template?
They use our template
* Business Associates. Are there multiple Business Associate Agreements to review? * Section 3.8 states 'This work will NOT include reviewing any of our Business Associate partners. However, we expect that you will review our Business Associate Agreements to verify they are in compliance' - Can you provide approximately how many Business Associate Agreements need to be verified? * How many business associate agreements will be reviewed? (RFP Section 3.8)
Unknown

* Page 6, 3.0 Scope of Work, Item 3.3, Privacy/Security. What is the size of these manuals for both HSC and DSS?
43 and 69 pages respectively.
* Do all other divisions conducting covered functions, as identified in Attachment C, adhere to the HSC or DSS HIPAA Privacy and HIPAA Security manuals?
Yes
* Are company policies and procedures standardized across the health care/CE and BA components of this assessment?
Policies within DSS are standardized based on the Federal regulations. BIT, as our Business Associate, is compliance with those as well.
* Are the IT and security team functions standardized across the health care/CE and BA components of this assessment?
As stated above, we standardize on the Federal requirements.
* Are there specific State cybersecurity requirements that need to be considered as part of this assessment?
No.

Technical Safeguards

* Has the Organization implemented a standard cybersecurity methodology e.g. NIST, ISO, SOC? * Are DSS currently having the Management/Technical & Operational controls in alignment with HIPAA compliance requirements?
Our overarching standard is NIST. However, various Federal agencies have their own detailed version of compliance for us to follow. For example, IRS; CMS; SSA; FBI and others.
* What security measures are currently used to safeguard ePHI. Are the controls configured and used properly?
DSS has a number of systems that host ePHI. They use a variety of technologies and hosting environments which impact the controls in place

* Can the Organization provide an overview of Access Controls procedures?
DSS has a number of systems that host ePHI. They use a variety of technologies and hosting environments which impact the controls in place.
* Description of Tools and Resources to manage the Technical Safeguards e.g. Azure, patching, Antivirus/Malware, Threat/Vulnerability management and end point protection and management * Does DSS have an enterprise risk management tool already in place, or a preferred tool/system for audit results and remediation tracking?
Such tools are under the control of BIT. They are in the process of adding an automated system to insurance compliance.
* When was the last Audit of User Activity performed? * How many risk items were identified as part of the Security Risk Assessment performed for just the Human Services Center?
503 items total were identified.
* Has the organization developed a standard practice for encrypting data in transit and at rest?
DSS has a number of systems that host ePHI. They use a variety of technologies and hosting environments which impact the controls in place.
* Is ePHI/EMR stored in Organization managed network/storage environment or is it a Cloud/SaaS based solution?
DSS has a number of systems that host ePHI. They use a variety of technologies and hosting environments which include BIT hosted, Cloud hosted, and SaaS.
* Does the organization have baseline configurations for all IT assets, with defined change management procedures?
DSS has a number of systems that host ePHI. They use a variety of technologies and hosting environments which impact the controls in place.
*Have you conducted penetration testing? *Should website penetration testing be included in the quote? (RFP Section 3.2.3.1.4.1) *When was the last Penetration test performed? *When was the last time risk assessment was performed by any third party/agency?
The last penetration tests were conducted in 2021

* Do you have a documented inventory of assets, technologies, databases? * Does DSS have current inventories, network diagrams, and data flow diagrams for which systems store or transmit ePHI? * Can you provide how many applications or information systems are in scope? * Will there be a certain number of in-scope systems/applications that will require a focused or detailed review of applicable security domain standards?
DSS has a number of systems that host ePHI. Quality of the documentation on these systems vary based system age and who maintains the system. The successful vendor will be given all the information that we have available. In your proposal you should outline your methodology for inventorying systems.

BIT Specific

* If the response does not include providing any software, can you validate that we do not need to include a completed Attachment E as part of our proposal? * Is Attachment E required as part of this submission? * RFP Questionnaire (Attachment E) pertains to software acquisition, implementation, and support. Is DSS anticipating software to be installed as part of the HIPAA Risk Assessment, or associated procedures? * Are we expected to complete and submit Attachment E?
If no software is being proposed, NA is an acceptable answer for Attachment E.
* Does DSS anticipate granting read access to systems for the contractor to obtain their own data?
DSS would provide access read access to system through the system interfaces.
* Does the Business Associate (BIT) understand their involvement in this process?
Yes
* Will the selected vendor be responsible for managing the Business Associate as well or will DSS manage any requests and questions we have for them?
There will be a Point of Contact (POC) with BIT that the vendor will work with. As needed the DSS POC can and will assist
* Does BIT support DSS in performing security mitigation / Implementing security controls for DSS ??

Yes, BIT would be the ones to do any work on the network or applications.
* Page 6, 3.0 Scope of Work, 3.7, Business Associate BIT. How large is the electronic environment of BIT? Specifically, what are: The number of Internet facing hosts comprising the internal and external environment (servers, routers, firewalls, IDS/IPS)? o # Servers in scope? o How many firewalls? o How may web sites? o IDS/IPS – do you utilize one and if so, is it locally managed? * Can you please provide the current number of infrastructure details (Physical Server, Virtual Server, Network Devices etc. * What is the aggregate Internet Capacity per location (<300mbps, <1gbps, <4gbps, up to 10gbps)? * How large is the IP space to be assessed (i.e., range size, how many class Cs, Class Bs, etc.)? Please provide the subnets/IP addresses? * How may hosts are in scope as part of this assessment (i.e., how many hosts are expected to be live out of the IP space)? * Approximately how many computer endpoints do you have (desktop PCs, laptops, servers)? * What is the size of the IT environment?
This information will not be shared without an agreement in place.
* How many staff in BIT that support the in-scope environment to be assessed? * What's your headcount of users (employees + contractors+interns)? What number/percentage of your workforce resides within organizational facilities? * How many staff in IT within DSS and HCS? * How many staff in security that support the in-scope environment to be assessed?
BIT staff are not specifically assigned to DSS but support all of State Government. As needed BIT staff can be tasked with helping in the audit.
* Are any segments of the in-scope electronic environment in a cloud environment?

* Do you manage your own data Center, or do you utilize any 3rd-party/colocation facilities? * Are there differences in cloud consumption between locations? * How much (%) of the infrastructure is in the cloud?
The State of South Dakota is in the process of moving our data storage and other services to the Cloud. This will be hosted in house. The environment will be the same at all locations. We are in the process of moving to the cloud but are not complete.
* Please provide from both an internal and external network perspective. * Can we request a high-level network diagram?
This information cannot be shared without an agreement in place.
* How many applications involved in the transmission, storage, and/or processing of ePHI across the scope?
There are five (5) public facing web applications. We do not have a definite count of the number of internal applications, but it would number in the dozens.
* How many Internet-facing sites/applications (URLs) are included in the scope?
There are five (5) public facing web applications.
* Would you like any applications tested?
Please include a description of how you test applications. Include a general cost estimate for testing.
* How many employees have remote access? * What number/percentage works remotely? * Any in-bound modems (or remote access) in use? How many users? * Specify the VLAN details how many are included in the Scope?
The number of employees who have Remote access is probably 500 who ***can*** use remote access. However, on any given day we probably have just a few dozen. Remote access is provided via Microsoft VPN, Netmotion, or Citrix Receiver.
* What database technologies are in use (Oracle, Microsoft SQL, IBM DB2, MySQL, PostgreSQL, etc.)?
Microsoft SQL is the State standard. DB2 on the mainframe? DSS has a number of vendor applications that can use other technologies.

* Is there a wireless environment to be assessed? **Yes**
* Are wireless networks in scope? **Yes**
  o What is the location of the facilities in scope (for wireless testing)? **Kneip and HSC**
  o What is the approximate size of the facilities in scope (e.g. sq. feet, number of floors, etc.)? **Kneip – 32,000 sq ft; HSC - 225,000**
  o How many access points are at each of the facilities? **Depends on location.**
  o How many ESSID are at each of the facilities? **Each facility shares the same ESSID**