

**Minnesota Department of Employment and Economic Development (DEED)
Project: Web Application Security Assessment**

DEED Answers to Vendor's Questions

Friday, 10 September 2010

1. Has data classification been completed on affected systems?
There is currently no data classification for the affected systems. The SOW would determine what specific data classification requirement for the affected systems.
2. What operating systems and code is running on the main frame systems?
Mainframe security is excluded from the SOW at this time.
3. What code has been used to write DEED applications?
The codes are .NET, ASP.NET, VB6.0, XML, VB.NET, JAVA, JAVA SCRIPT, Servay SCRIPT, PERL, DreamWeaver, TopStyle, POPCharts, SQL Srv, LDAP Query, Access2k, and E-mail Outlook.

The updated BIT-APP Portfolio identifies what code was used to develop each of the 82 applications supported on the new SQL2008 environment. There may be additional applications that BIT supports that do not use our SQL2008 enterprise platform that will need to be added to this list. There are additional 10 apps that are listed on the non-enterprise SQL environment.

4. How many dynamic pages are in each application?
Varies between 2 to 1,000 dynamic pages.

How many different roles are assigned to each application?

Varies between 2 to 200 roles. DEED uses role based security for access to data for apps and reports, there are roughly 200 security roles defined within the largest app.

5. Section 2b requests: 'Supply previous client engagement information related to application classification and risk assessments, vulnerability assessment and application vulnerability assessment documents, also please expunge prior clients and sensitive information'. Can you please clarify if you are asking for sanitized deliverables or are you asking for case study descriptions of similar projects? **DEED would like to review vendor's sanitized documents related to past or current web application assessments.**
6. Please confirm if this will be a fixed bid contract or a T&M contract. Section 3c requires submission of hourly rate and total estimated hours for each staff member that will be assigned to the project. Yet, on page 3 the Contract Type is listed as a fixed bid contract.
The Web Application Security Assessment SOW is a fixed bid.
7. Can DEED accommodate a team of several consultants?
Yes, DEED can accommodate about 2 or 3 consultants.

8. What requirements documentation exists around the CIA for the in scope data and applications? **No current DEED document exists related to data classification consistent with CIA. However, DEED utilizes three Minnesota State classifications – see below:**
- **Public data**: We must give public data to anyone who asks; it does not matter who is asking for the data or why.
 - **Private data**: We cannot give private data to the general public, but you have access when the data is about you. We can share your private data with you, with someone who has your permission, with DEED staff who need the data to do their work, and with others as permitted by law or court order.
 - **Confidential data**: Confidential data has the most protection. We cannot give members of the public any access to confidential data about you. Nor can we give you direct access to confidential data even when the confidential data is about you. We can share confidential data about you with DEED staff who need the data to do their work and to others as permitted by law or court order.
9. While frameworks and best practices can be used to create many of the “expected controls” It would be best if DEED can provide their specific requirements where applicable, so the end results is a best practices driven approach augmented with DEED specific requirements as needed. **DEED desires to meet the intent of NIST 800-53 and 800-30 Regulations to safeguard and protect data.**
10. When and in what format can DEED provide documentation on the current security controls? **DEED can provide PDF versions of policy.** Typically this would include:
- a. Policies that drive the overall approach to security. **DEED Information Security Policy and DEED General Information Security Standard Manual.**
 - b. Process flows / work flows that outline how day to day business and change management operate within the framework of the stated policies. **The DEED change management process is in the draft deployment stage.**
 - c. An auditable trail of systems use and change management that allows the ability to validate adherence to the policies. **The DEED change management process is in the draft deployment stage.**
 - d. A current network diagram of the DEED datacenter and the mainframe network connections. **Mainframe security is excluded from the SOW at this time.**
11. Does DEED have a current data classification policy or standard? **See question 8 for answer.** If so please provide information on the classification tiers? **See question 8 for answer.** If not, do paragraphs I.a) and I.b) imply that the project would create such a classification scheme? **See question 1 for answer.**
12. Can DEED provide a data-catalog. for the PII that they interact with? **DEED does not have a data catalog available** (Or a description of the data types considered PII) **See questions 8 and 9 for answers.**

13. Is there a CMDB or Sources of Truth for the systems, applications, services, and data types that will be in scope for this project? **DEED does not have a current formal and complete CMDB system. However, we do possess a partial CMDB focused specifically on Databases (40) and Applications (82) hosted on our SQL2008 enterprise server platform which comprises the bulk of our supported critical web application services. However, there are additional 10 apps that are listed on the non-enterprise SQL environment.**
- If not what type of mapping of PII to systems and services will DEED be providing?
None
14. Questions on the project scope:
- Does the scope include all web based systems and all dependencies of these systems? **Does not include all dependencies.**
 - Is the evaluation to include both internal and external access to these systems. **Yes, the SOW assessment includes both internal and external web applications.**
 - Deliverable III a – i states “Summary of the scope and processes tested” Is DEED leaving the scope and processes to be tested to the external consultants, or will the scope and chosen processes be arrived at in consultation with the DEED SMEs?, **The scope is based upon the approximate 82+ (internal & external) web based applications hosted on SQL enterprise environment. However, there are additional 10 apps that are listed on the non-enterprise SQL environment. Review DEED’s Statement of Work on first page of document related to process to be tested in accordance with DEED’s approval and consent.**
 - Can you provide information on the specifics as to type, size, OS version, Network Stack and Network connectivity of the Mainframe environment in IV? **NA** Will a SME resource be available for the mainframe environment? **Mainframe security is excluded from the SOW at this time.**
15. Redundant / Non-production systems.
- Are there relevant and representative Development or Stage environment for all of the systems to be evaluated for this project? **Yes for both development and stage.** (Aggressive vulnerability and penetration testing can have detrimental impacts to systems and all tests should be validated against representative non-production systems to gauge the risks before investigating production systems) **DEED supports the following four environments for application development through production: Development, QA/Test, Stage, Production environments—Note that not applications require all four environments.**
16. Scope of the documentation.
- Can you please speak to the user audience, level of technical detail, and level of user familiarity with the systems for each set of users which will require a “security educational material pamphlet template”? **Security awareness is excluded from the SOW at this time.**
 - Can you please define the “application resource allocation project” is this a CMDB or Source of Truth for all applications at DEED? **NA** What type of system or tool does this project utilize and how may we link to it? **NA** (Is it also managed in SharePoint?)
No. see section 13
 - The SOW states

- i. *“Vendor is expected to create specific technical implementation controls, mitigation activities and documentation for DEED-wide with specific emphasis OLA DEED audit findings starting from phase I through IV below.”*

However the deliverables for phase I-IV mention only reports and an educational template (please see questions on the template(s) below) Could you please clarify the type, and level of detail of documentation required for this project? **Security awareness is excluded from the SOW at this time.**

- 17. Can you speak to your off site backup and DR strategy and it’s role in this project? **DEED manages an off-site backup program. The DEED DR strategy is out of scope for this SOW.**
- 18. Does your access controls approach include federation? **No, DEED does not deploy federation technologies.** If so, is DEED initiating or receiving? **NA** What is the number of different domains? **NA**
- 19. Could you please clarify what this statement means: DEED will NOT be conducting a reverse auction for this SOW. **The term refers that DEED will not obtain a contract for the lowest bidder.**

Application Classification and Risk Assessment (All DEED Enterprise Applications)

- 20. Will DEED provide a listing of the applications included in the scope of this assessment? **Yes, DEED will provide a listing of all web based applications prior to the assessment. See section 13**
- 21. Will DEED provide the classification labels used in the CIA assessment? **Examples include Priority 1 through 5. Attached below is the Office of Enterprise Technology Enterprise Risk Management Matrix and definitions.**

Information System Priority Rating			
Business Process/Service Priority Level	Impact to Information Asset		
	High Impact	Moderate Impact	Low Impact
Priority 1	Priority 1	Priority 2	Priority 3
Priority 2	Priority 2	Priority 3	Priority 4
Priority 3	Priority 3	Priority 4	Priority 4
Priority 4	Priority 4	Priority 4	Priority 4

Information System Priority Assignment Matrix

The model will be utilized during the SOW assessment.

DEED has prioritized its services based on the following priority level definitions established:

Priority 1 (Immediate threat to public health and/or safety)
 Activities that must remain uninterrupted. Generally, these would include agencies and facilities that operate 24 hours a day. For instance, patient care at regional treatment centers or nursing care facilities, correctional facility operations and fire suppression, law enforcement, emergency medical operations are examples of priority one services. A process for maintaining communication with agency personnel and the Pandemic Influenza Executive Committee is also considered a Priority 1 service.

- **Priority 2 (Disorder or an economic impact may develop if not delivered in a few days)** Activities with a recovery time objective of 25 hours to 5 days that can be disrupted temporarily or might be periodic in nature, but must be re-established within a few days. For example, investigations, regulation enforcement, and benefit payments to individuals would generally be considered priority two services. In most cases, agency support services such as communication, purchasing, human resources and payroll are considered Priority 2.
 - **Priority 3 (Services required by law or rule that can be suspended by law or rule during an emergency).** Activities with a recovery time objective of 6 days to 30 days that can be disrupted temporarily but must be re-established sometime before the pandemic wave is over (<6 weeks). For example, license renewals, vehicle registration, and recording land transactions would generally be considered Priority 3.
 - **Priority 4 (Services that could be suspended during an emergency and are not required by law or rule)** Activities with a recovery time objective of 30+ days which can be deferred for the duration of a pandemic influenza wave (6-12 weeks). For example, educational programs, training and general maintenance programs would generally be considered priority 4 services
22. Will the definitions be provided for the classification labels listed in question 2 above or do the definitions need to be determined as part of the project? **See question 9 for answer.**
23. Is there a preferred common body of knowledge that should be used for determining the set of expected controls? **See question 9 for answer.** If so, what is the common body of knowledge? **Yes, see question 9 for answer.**
24. Will DEED provide the expected format for the MS Excel spreadsheet? **Yes, DEED would expect the vendor's data output format as Microsoft's Excel and recommend a database schema.** What database is used for reporting? **SQL2008-SSRS**

Vulnerability Assessment of DEED IT Environment (All DEED applications containing PII)

25. Please describe in more complete detail the expectations of this vulnerability assessment regarding scope, expected procedures, etc. **Review the DEED Statement of Work on first page of document.**
26. Approximately how many applications could be considered for this assessment? **Approximately 82+ web based applications (internal and external).**
27. Is this assessment similar to an IT general controls review? **NA**

Application Vulnerability Assessment (All DEED applications containing PII)

28. Approximate the number of web applications that will be assessed during this phase. **See question 9 for answer.**
29. Will there be a separate report for each application? **Yes, a separate report per application is required because of application complexities and different levels of controls.** Or one report segmented by application? **Yes**

30. Mainframe and Security Awareness Material - **Mainframe security and security awareness are excluded from the SOW at this time.**

- a. Identify the mainframe(s) that are in scope. **NA**
- b. Describe the expectations of the scope for the mainframe security assessment. Does it include technical testing as well as administrative and physical controls testing? **NA**
- c. Is MS Powerpoint acceptable for delivery of the training and education material? **NA** If not, what is the expected format? **NA**
- d. Will the vendor selected be presenting the material? **NA**