Attachment K

DOR SECURITY LANGUAGE

FOR TECHNOLOGY SERVICES THAT CONTAIN FTI

ALL REQUESTS FOR PROPOSALS (RFP), QUESTIONS (RFQ), AND INFORMATION (RFI)

BACKGROUND

DOR complies with IRS Publication (PUB) 1075 security requirements to protect the Federal Taxpayer Information that it handles and stores. IRS PUB 1075 is based on National Institute of Standards and Technology (NIST) security guidance. When vendors, contractors, and other external organizations partner, support, and conduct business with DOR, they must also comply with (a) IRS PUB 1075 and NIST security requirements. Compliance with these requirements means that they must document and perform work according to IRS PUB 1075 and NIST security standards. It also means that vendors and contractors will be audited against those standards.

SECURITY LANGUAGE

Security Requirements

DOR has adopted a FISMA-based security requirement for its operations and systems due to the high need to keep DOR’s data confidential, available, and with high integrity. DOR uses the highest intolerance for risk in its assessment of the system. DOR requires that the respondent be compliant with such a security scheme for its system and operations because DOR will be transmitting its data to the respondent. The following points detail DOR’s requirements. PLEASE NOTE: DOR will not accept any respondent solution that does not meet DOR’s security requirements.

1. Respondents must comply with NIST and IRS Publication 1075 (PUB 1075) security controls and requirements to which DOR subscribes. DOR has adopted the NIST 800-53 standards for security controls. Respondents must be familiar with the requirements of NIST 800-53 to certify that their software conforms to NIST 800-53 and to assist DOR with installing its software in a manner that complies with NIST 800-53. Respondents must also comply with all aspects of NIST 800-53 during support activities when they attach to the State’s data network to perform support tasks. Any respondent who possesses DOR data in their facilities must comply with all aspects of NIST 800-53 pertaining to safeguarding that data. Respondents should also note that in some instances NIST 800-53 references other federal standards, such as the FIPS 140-2 Encryption Standard, with which they must also comply. DOR must comply with IRS PUB 1075 governing federal, state, and local entities’ use of federal tax information (FTI). As a result, the respondent must also comply with IRS PUB 1075 when handling FTI and the systems on which it resides. The respondent should note that PUB 1075 is a subset of the standards and controls identified in NIST 800-53.

DOR will evaluate all system security models based on DOR’s reading of FISMA, NIST SP800-53, and security best practices.

It is DOR’s security standard that each system is responsible for securing its own data and should not rely on environmentally supplied technologies for security. For example, a respondent should not assume that the data in their system is secure because DOR has secured the servers upon which the application or its database is installed. Under this assumption, the data in the respondent’s system is immediately vulnerable to intrusion if the intruder breaks through DOR’s server security. The respondent recognizes that compliance with DOR’s security standard is vital to DOR’s ability to protect against unauthorized access or intrusion.

A. The respondent shall provide evidence of compliance with NIST 800-53 and IRS PUB 1075. Evidence shall include the report of the respondent’s self-assessment of information technology (IT) assets, processes, practices, and facilities against security criteria from aforementioned documents. The first of these self-assessments shall be provided with the RFP response. This assessment should be qualitative in nature. The respondent should review the aforementioned publications and provide their compliance with each point.

B. The respondent must certify to compliance with DOR’s reading of FISMA, NIST SP800-53, and security best practices.

C. The respondent must describe how its proposed solution provides its own data security.

D. The respondent will be required to evaluate its proposed system against a set of security technology implementation guidelines (STIGs). The STIGs are specific to the respondent’s technology stack that was described in section technical proposal. They are also a very objective measure of compliance with NIST requirements. The STIGs are available on the Defense Information Security Agency (http://iase.disa.mil/stigs) website. The respondent must supply DOR with a copy of its technical architecture as a part of the RFP response. DOR will review the technical architecture and provide the respondent with a STIGs checklist to complete prior to orals.

2. The respondent acknowledges that the information that DOR provides may include personally identifiable information and it is the respondent’s obligation to keep all such accessed information confidential and secure. Accordingly, the respondent shall purge all information received from DOR at the end of the calendar year in which the data was received, provided that DOR and Contractor may extend such period if and solely to the extent such information is retained thereafter in archival form to assist DOR or Contractor in performing statistical analysis required for DOR’s or Contractor’s legal or regulatory compliance efforts

3. The respondent certifies that the data processed during the performance of this contract will be completely purged from all data storage components of the respondent’s computer facility at the end of the calendar year in which the data was received except for data needed for legal or regulatory compliance purposes. Such data shall be protected in accordance with the contract’s security requirements. The respondent certifies that any confidential taxpayer information and data remaining in any storage component pending such purge will be safeguarded to prevent unauthorized disclosures.

4. In the event of an information disclosure or technical security incident, DOR security must be informed within 24 hours of the incident along with relevant details about: (1) the indications and warnings of compromise were observed; (2) what and when information and systems were potentially compromised; and (3) the mitigating actions taken and planned to protect against and recover from the potential compromise. The DOR Security Team will provide specific details to the selected respondent.

5. The respondent will follow the IRS Safeguard Exhibit 7 as follows:

**I. PERFORMANCE**

In performance of this contract, the Contractor agrees to comply with and assume responsibility for compliance by Contractor’s employees with the following requirements:

1. All work will be performed under the supervision of the contractor or the contractor's employees.
2. The contractor and the contractor’s employees with access to or who use FTI must meet the background check requirements defined in IRS Publication 1075.
3. Any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Disclosure to anyone other than an officer or employee of the contractor is prohibited.
4. All returns and return information will be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output will be given the same level of protection as required for the source material.
5. The Contractor certifies that the data processed during the performance of this contract will be completely purged from all data storage components of Contractor’s computer facility, in accordance with the terms of its document retention/ destruction policies for such data (excluding longer storage periods needed for legal or regulatory compliance purposes).. If immediate purging of all data storage components is not possible, the Contractor certifies that any IRS data remaining in any storage component will be safeguarded to prevent unauthorized disclosures.
6. Any spoilage or any intermediate hard copy printout that may result during the processing of IRS data will be given to the agency or the agency’s designee. When this is not possible, the Contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts, and will provide the agency or the agency’s designee with a statement containing the date of destruction, description of material destroyed, and the method used.
7. All computer systems receiving, processing, storing or transmitting FTI must meet the requirements defined in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operational, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to Federal Tax Information.
8. No work involving Federal Tax Information furnished under this contract will be subcontracted without prior written approval of the IRS.
9. The contractor will maintain a list of employees authorized access. Such list will be provided to the agency and, upon request, to the IRS reviewing office.
10. The agency will have the right to void the contract if the contractor fails to provide the safeguards described above.

**II. CRIMINAL/CIVIL SANCTIONS**

1. Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that returns or return information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such returns or return information for a purpose or to an extent unauthorized herein constitutes a felony punishable upon conviction by a fine of as much as $5,000 or imprisonment for as long as five years, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized future disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than $1,000 with respect to each instance of unauthorized disclosure. These penalties are prescribed by IRCs 7213 and 7431 and set forth at 26 CFR 301.6103(n)-1.
2. Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Inspection by or disclosure to anyone without an official need-to-know constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as $1,000.00 or imprisonment for as long as 1 year, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized inspection or disclosure of returns or return information may also result in an award of civil damages against the officer or employee [United States for Federal employees] in an amount equal to the sum of the greater of $1,000.00 for each act of unauthorized inspection or disclosure with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure plus in the case of a willful inspection or disclosure which is the result of gross negligence, punitive damages, plus the costs of the action. The penalties are prescribed by IRCs 7213A and 7431.
3. Additionally, it is incumbent upon the contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.
4. Granting a contractor access to FTI must be preceded by certifying that each individual understands the agency’s security policy and procedures for safeguarding IRS information. Contractors must maintain their authorization to access FTI through annual recertification. The initial certification and recertification must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, contractors must be advised of the provisions of IRCs 7431, 7213, and 7213A (see Exhibit 4, *Sanctions for Unauthorized Disclosure*, and Exhibit 5, *Civil Damages for Unauthorized Disclosure*). The training provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. (See Section ) For both the initial certification and the annual certification, the contractor must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

**III. INSPECTION**

The IRS and the Agency shall have the right to send its officers and employees into the offices and plants of the contractor for inspection of the facilities and operations provided for the performance of any work under this contract for compliance with requirements defined in IRS Publication 1075. The IRS’ right of inspection shall include the use of manual and/or automated scanning tools to perform compliance and vulnerability assessments of information technology (IT) assets that access, store, process or transmit FTI. On the basis of such inspection, specific measures may be required in cases where the contractor is found to be noncompliant with contract safeguards.