

Foundation Cloud Hosting Services

(FCHS)

Information Technology

Security and Privacy Requirements

for

U.S. Department of the Interior

FCHS IT SECURITY AND PRIVACY REQUIREMENTS

V1.2

Table of Contents

[1. Background 3](#_Toc336000831)

[2. Applicable Laws, Policy, Rules, Regulations, Standards and Guidelines 4](#_Toc336000832)

[3. Information Security and Privacy Requirements 9](#_Toc336000833)

[4. Personnel Security Background Investigations and Clearances 11](#_Toc336000834)

[5. Non-Disclosure Agreements (NDAs) 12](#_Toc336000835)

[6. Personnel Changes 12](#_Toc336000836)

[7. Government access 12](#_Toc336000837)

[8. Incident Detection, Notification, Handling, Response, Containment, Eradication, Recovery and Reporting 13](#_Toc336000838)

[9. Federal Information Security Management Act (FISMA) 14](#_Toc336000839)

[10. Assessment and Authorization (A&A) 15](#_Toc336000840)

[11. Government support of the FISMA Assessment and Authorization (A&A) Process 16](#_Toc336000841)

[11.1 System Security Plan (SSP) 16](#_Toc336000842)

[11.2 Continuous Monitoring Plan (CMP) 17](#_Toc336000843)

[11.3 Contingency Plan (CP) 19](#_Toc336000844)

[11.4 Security Assessment Plan and Report (SAP/SAR) 19](#_Toc336000845)

[11.5 Plan of Action and Milestones (POA&M) 20](#_Toc336000846)

[11.6 Information Assurance (IA) Requirements 20](#_Toc336000847)

[11.6.1 Cloud Service Delivery Model Security Requirements 21](#_Toc336000848)

[11.6.2 Independent Verification and Validation (IV&V) 27](#_Toc336000849)

[11.6.3 Internet Logon Banner 27](#_Toc336000850)

[11.6.4 Logon Warning Banner 28](#_Toc336000851)

[11.6.5 Quality Control (Malicious Code) 28](#_Toc336000852)

[11.6.6 Security Controls 28](#_Toc336000853)

[11.6.7 Training 28](#_Toc336000854)

[11.6.8 Privacy 29](#_Toc336000855)

[12. Roles and Responsibilities 29](#_Toc336000856)

[13. IT Security Policies, Standards, Guidelines and Other Publications 30](#_Toc336000857)

APPENDIX A - [IT Security and Privacy Checklist 32](#_Toc336000859)

APPENDIX B - [Deliverable and Reporting Requirements 33](#_Toc336000861)

1. Background

The Department of the Interior (DOI) is seeking Foundation Cloud Hosting Services (FCHS) that can meet security control objectives for IaaS, PaaS and SaaS information systems having an overall security categorization of “LOW”, “MODERATE” or “HIGH”, commensurate with the DOI hosted applications, and corresponding individual potential risk impact ratings of “LOW”, “MODERATE” or “HIGH” for the Confidentiality, Integrity and Availability objectives with corresponding management, operational, and technical security controls to adequately protect sensitive agency information, the information system(s) and operating environments employed in the operations and maintenance of the delivery of those services.

As with all Federal government agencies, DOI is subject to numerous requirements stemming from a variety of Laws, rules, regulations, directives, and standards aimed at ensuring the protection of sensitive agency information and information systems. These requirements include providing information security protections commensurate with the risk and magnitude of the potential harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of (i) information collected or maintained by or on behalf of the agency; and (ii) information systems used or operated by the agency or by a contractor on behalf of the agency.

Consequently, the Contractor shall also adhere to and comply with applicable Laws, Executive Orders and Executive Branch Policy regarding the design, build, testing, operations and maintenance of the information system and the security controls designed to safeguard agency information. This document establishes the information technology (IT) security and privacy requirements in which the service provider must comply. These requirements are applicable when DOI information is generated, accessed, stored, processed, or exchanged with DOI or on behalf of DOI by a service provider or subcontracted service provider, regardless of whether the information resides on a DOI information system or a service provider/subcontracted service provider’s information system. The service provider shall protect the confidentiality, integrity, and availability of DOI electronic information and IT resources and protect DOI electronic information from unauthorized disclosure.

DOI remains responsible and accountable for all risk incurred by use of services provided by external service providers. This risk is addressed by requiring a minimum set of security and privacy controls that must be implemented and monitored to provide assurance that DOI information remains accurate, secure and available. The requirements outlined herein are intended to provide DOI with an acceptable level of trust and controls that must be maintained throughout the lifecycle of the acquisition. This level of trust and controls are maintained by:

1. Reciprocity through a centralized, Federal acquisition vehicle in accordance with the Federal Risk and Authorization Management Program (FedRAMP). In accordance with the OMB memorandum entitled, *Security Authorization of Information Systems in Cloud Computing Environments*, issued on December 8, 2011, the DOI Authorizing Official (AO) anticipates leveraging and accepting provisional authorizations granted by the FedRAMP Joint Authorization Board (JAB), comprised of the Department of Defense (DOD), Department of Homeland Security (DHS) and the General Services Administration (GSA), in granting security authorizations and an accompanying authority to operate (ATO) for DOI use of the FCHS, to the extent available. DOI does not necessarily anticipate leveraging authorizations granted independently by other individual agencies, but may opt to do so at its discretion;
2. The Provider acquiring the services of an agreed upon independent third-party assessor to test and evaluate the effectiveness of the applicable security controls; and
3. Meeting the IT security and privacy requirements set forth within this document, including satisfying the ongoing requirements identified within the *IT Security and Privacy Checklist (Appendix A)* and eighteen *DOI Security Control Standards* that correspond to the National Institute of Standards and Technology (NIST) Special Publication (SP) 80-53, *Recommended Security Controls for Federal Information Systems,* which identify additional required control enhancements.

2. Applicable Laws, Policy, Rules, Regulations, Standards and Guidelines

At no additional cost to the Government, Offeror shall comply and cause its Provider or subcontractor to agree to comply with all Information Assurance, IT security and privacy laws, regulations, policies and standards that are applicable to Offeror and Provider in their provision of the services to the Government. In addition, Offeror shall agree and Offeror shall cause Provider or subcontractor to agree, to assist the Government in its compliance with the requirements set forth in the Federal Information Security Management Act (FISMA), by successfully completing the Assessment and Authorization (A&A – formerly referred to as Certification and Accreditation (C&A)) required by FISMA, Office of Management and Budget (OMB) policy, and NIST standards for all information systems provided by Offeror and Provider or subcontractor that shall be used in the provision of the Solutions. Offeror shall ensure that Provider or subcontractor shall complete the A&A process on or before providing solutions on-boarding notice. If, during the term of this contract, there are changes to the data protection and privacy laws and regulations, including FISMA, or if there are new US Federal Government requirements applicable to the Government, then the Offeror and the Government will address these changes in a mutually agreed upon Change Management Process.

A number of laws, regulations, directives, policies, standards and guidelines mandate protection of Federal government information, information systems and related resources, including all information systems owned or operated on behalf of the government by the Contractor/Provider. Applicable laws passed by Congress include:

| Authority | Description |
| --- | --- |
| Federal Records Act of 1950, 44 U.S.C. §§21, 29, 31 and 33 | Establishes the framework used by Federal agencies for their Records Management programs. |
| The Freedom of Information Act (FOIA) of 1966, 5 U.S.C. § 552 | This law requires that Federal information be made available to the public except under certain specified conditions. |
| The Privacy Act of 1974, 5 U.S.C. § 552a | This law imposes collection, maintenance, use, safeguard, and disposal requirements for Executive Branch offices maintaining information on individuals in a “system of records.” |
| Federal Managers Financial Integrity Act of 1982 (FMFIA), 31 U.S.C. § 3512 | This law mandates that Federal agencies establish and maintain an internal control program to safeguard data processing resources, assure their accuracy and reliability, and protect the integrity of information resident on such systems. |
| Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030 | This law provides for the punishment of individuals who access Federal computer resources without authorization, attempt to exceed access privileges, abuse government resources, and/or conduct fraud on government computers. |
| Government Performance and Results Act (GPRA) of 1993, 31 U.S.C. § 1101 | This law establishes policies for managing agency performance of mission, including performance of its practices. |
| Paperwork Reduction Act of 1995, Revised, 44 U.S.C. §§ 3501-3520 | This law provides for the administration and management of computer resources. |
| Clinger-Cohen Act – Information Technology Management Reform Act of 1996, 40 U.S.C. § 1401 et seq. | This law improves the acquisition, use, and disposal of Information Technology (IT) by the Federal government. |
| Federal Financial Management Improvement Act (FFMIA) of 1996, 31 U.S.C. § 3111 | This law mandates Federal agencies to implement and maintain financial management systems that comply substantially with Federal systems requirements, Federal accounting standards, and the U.S. Government Standard General Ledger (SGL). FFMIA also requires GAO to report annually on the implementation of the act. |
| National Information Infrastructure Protection Act of 1996, 18 U.S.C. § 1030 | This law provides for the protection of computer resources. |
| Government Paperwork Elimination Act (GPEA) of 1998,  44 U.S.C. § 3504 | This law provides for Federal agencies, by October 21, 2003, to give persons who are required to maintain, submit, or disclose information, the option of doing so electronically when practicable as a substitute for paper and to use electronic authentication methods to verify the identity of the sender and the integrity of electronic content. |
| E-Government Act of 2002, 44 U.S.C. § 101 | This law enhances the management and promotion of electronic government services and processes by establishing a broad framework of measures requiring technology to enhance citizen access to government information services. |
| Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. § 3541 | FISMA requires Federal agencies to establish agency-wide risk-based information security programs that include periodic risk assessments, use of controls and techniques to comply with information security standards, training requirements, periodic testing and evaluation, reporting, and plans for remedial action, security incident response, and continuity of operations. |

The following are Executive Orders that provide details related to information security for Federal Agencies.

|  |  |
| --- | --- |
| Executive Order 10450, Security Requirements for Government Employees, April 1953 | This order establishes that the interests of national security require all government employees be trustworthy, of good character, and loyal to the United States. |
| Executive Order 13011, Federal Information Technology, July 1996 | This order establishes policy for the head of each agency to effectively use information technology to improve mission performance and service to the public. |
| Executive Order 13103, Computer Software Piracy, September 1998 | This order establishes policy that each executive agency shall work diligently to prevent and combat software piracy in order to give effect to copyrights associated with computer software. |
| Presidential Decision Directive 63: Critical Infrastructure Protection, May 1998 | This directive requires that the United States take all necessary measures to swiftly eliminate any significant vulnerability to both physical and cyber attacks on critical infrastructures, including our cyber systems. |
| Executive Order 13231, Critical Infrastructure Protection in the Information Age, October 2001 | This order establishes policy that ensures protection of information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such information systems. |

The following are Executive branch policies established through directives published by OMB based on the applicable laws passed by Congress.

| OMB Circular | Description |
| --- | --- |
| A-11, Section 53, Information Technology and E-Government | This directive specifies the identification of security and privacy safeguards for managing sensitive information. |
| A-123, Management Accountability and Control, as revised December 21, 2004 | This directive specifies the policies and standards for establishing, assessing, correcting, and reporting on management controls in Federal agencies. |
| A-127, Financial Management Systems, as revised by Transmittal Memorandum Number 3, December 1, 2004 | This directive prescribes policies and standards for executive departments and agencies to follow in developing, operating, evaluating, and reporting on financial management systems. |
| A-130, Appendix I, Federal Agency Responsibilities for Maintaining Records About Individuals | This directive prescribes policy to agencies for the implementation of the Privacy Act and reporting requirements related to the management of personally identifiable information (PII). |
| A-130, Appendix III, Security of Federal Automated Information Resources, as revised by Transmittal Memorandum Number 4, November 28, 2000 | This directive stipulates that each agency shall implement a comprehensive automated information security program. The appendix establishes basic managerial and procedural controls that shall be included in Federal automated information systems. |

The Contractor shall also ensure conformance and compliance with, and provide services that implement and meet, the following requirements:

* OMB Memorandum M-05-24, *Implementation of Homeland Security Presidential (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors.*
* OMB Memoranda M-06-16, [*Protection of Sensitive Agency Information*](http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2006/m06-16.pdf), and [M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*](http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2007/m07-16.pdf), which establish requirements for the use of two-factor authentication for remote system access and requirements for responding to breaches or possible breaches of Personally Identifiable Information (PII).
* OMB Memorandum M-08-05, *Implementation of Trusted Internet Connections*, which establishes the requirement for DOI to comply with the Trusted Internet Connection (TIC) initiative and the architectural requirements defined by the Department of Homeland Security (DHS) in the TIC Reference Architecture (current version 2.0 dated 2011).
* OMB Memorandum M-08-16, *Guidance for Trusted Internet Connection Statement of Capability Form.*
* Office of Management and Budget (OMB) Memorandum M-08-26, *Transition from FTS 2001 to Networx.*
* OMB Memorandum M-08-27, *Guidance for Trusted Internet Connection Compliance.*
* OMB Memorandum M-11-11, *Continued Implementation of Homeland Security Presidential Directive (HSPD) 12– Policy for a Common Identification Standard for Federal Employees and Contractors.*
* OMB [M-11-33, *FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*](http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-33.pdf).
* National Security Presidential Directive and Homeland Security Presidential Directive (NSPD-54/HSPD-23), *Comprehensive National Cyber Security Initiative.*
* Homeland Security Presidential Directive (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractors*.
* Department of Homeland Security (DHS) Trusted Internet Connection (TIC), Version 2.0, Reference Architecture requirements.
* Federal Identity, Credential and Access Management (FICAM) Roadmap and Implementation Guidance and associated NIST standards regarding implementation and use of HSPD-12 Personal Identity Verification (PIV) two-factor SmartCard Public Key Infrastructure (PKI) based credentials for logical authentication.
* NIST Federal Information Processing Standard (FIPS) Publications.
* NIST 800-series Special Publications (SP).
* NIST Security Technical Implementation Guides (STIGs – also referred to as security configuration checklists).
* All management, operational and technical security control and continuous monitoring requirements as specified by FedRAMP.
* DOI TIC security architecture.
* DOI IT security and privacy policies, standards, guidelines and procedures to include, but not limited to, the following:
  + DOI Departmental Manual (DM) 375DM19;
  + DOI Security Control Standards (i.e., the eighteen (18) DOI-specific security control family standards based on the NIST SP 800-53 security control families that include agency-wide standard parameters, values, etc. for certain controls and that incorporate additional controls or control requirements for implementations within cloud computing environments; and
  + DOI-specific standards, procedures and security requirements specified in the following:
    - DOI Plan of Actions and Milestones (POA&M) Process Standard;
    - DOI Computer Security Incident Response Handbook and associated incident notification, response, handling and reporting requirements;
    - Privacy Loss Mitigation Strategy (PLMS) and associated Breach Incident Reporting and Handling Procedures; and

3. Information Security and Privacy Requirements

Service providers are required to comply with the security and privacy requirements summarized in this section and identified in the *IT Security and Privacy Checklist (Appendix A)*, NIST standards and the *DOI Security Control Standards* established using the NIST SP 800-53*.* Allapplicable security and privacy controls identified herein, and in the *DOI Security Control Standards,* shall be assessed in accordance with the NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations.*

The level of compliance with the required minimum baseline security and privacy controls are determined by DOI to ensure a level of trust with the service provider and that the risk from using external services is at an acceptable level to the DOI authorizing official.

* **Security and Privacy Requirements.** DOI requires that the service provider implement the security controls identified herein, in the *IT Security and Privacy Checklist (Appendix A)* and in the *DOI Security Control Standards,* to ensure the confidentiality, integrity, and availability of DOI information. A summary of some of the key security requirements is as follows:
* Under some circumstances, the use of public or hybrid clouds and their associated risks may be deemed acceptable by the DOI Authorizing Official (AO) who shall make the risk-based determination in consultation with, and with the concurrence of, the Department’s Chief Information Officer (CIO). DOI is not aware of public or hybrid cloud solutions at this time that would meet the security requirements defined in this solicitation, federal policy, and individual task orders for “MODERATE” systems, but may become aware of these through the solicitation process or otherwise in the future. DOI does not wish to preclude potential interagency customers from implementing hosting in public or hybrid cloud solutions based upon their independent risk management processes, or to preclude hosting of moderate systems in public or hybrid clouds if, and when, the specific security requirements defined in the RFP and the individual Task Orders can be met.

* + All service provider information system components that access, store, transmit and/or process DOI information must be located within the sole jurisdiction of the United States Federal Government (i.e., within the continental United States, Hawaii, Alaska, Puerto Rico, Guam, and/or the Virgin Islands);

* + Trusted Internet Connection 2.0 - The IaaS, PaaS and SaaS must provide a Trusted Internet Connection 2.0 (TIC 2.0, see <http://www.dhs.gov/files/programs/gc_1268754123028.shtm> ) compliant interconnection architecture.
  + IPv6 - The IaaS, PaaS and SaaS must comply with federally mandated IPv6 requirements (see <http://www.cio.gov/documents/IPv6memofinal.pdf> ).
  + Identity, Authorization and Access Management (IdAAM) - The IaaS, PaaS and SaaS must seamlessly integrate with the DOI IdAAM solution that consists of the Microsoft Active Directory (AD) and Public Key Infrastructure (PKI) architecture and associated Certificate Authority and DOI HSPD-12 PIV SmartCard-based credentials and enable logical authentication utilizing those credentials without requiring additional Contractor solution credentials. DOI uses Microsoft’s Active Directory to create a single DOI-Wide directory of all users. This directory is known as the Enterprise Active Directory (EAD). The FCHS IaaS, PaaS and SaaS must recognize the EAD as the authoritative source for authentication. DOI currently utilizes name and password authentication, however the Department is transitioning to Entrust PKI for authentication. The IaaS, PaaS and SaaS shall support authentication using DOI’s Entrust PKI. It is envisioned that in the future all users will authenticate with the Entrust PKI and use the HSPD-12 PIV Smart Card; for the present some users will continue to be authenticated by user name and password, and this method must also be supported.
  + DOI must be granted access to service provider facilities in legal, chain of custody scenarios that may arise and upon request to ensure that an acceptable level of trust is maintained;
  + All service provider personnel must undergo background investigation, performed by the Office of Personnel Management, prior to being granted logical or physical access to DOI information; and
  + The service provider will share all DOI information with DOI using an agreed upon secure transmission method to ensure the security of DOI information.
* **Security Assurance Requirements.** DOI requires that the service provider develop a Security Assessment Plan and initially assess all applicable security controls, using an agreed upon independent third-party assessor, andprovide security assessment results in a Security Assessment Report for all applicable security controls (identified herein, in the *IT Security and Privacy Checklist (Appendix A)* and in the *DOI Security Control Standards)*, including an appropriate characterization and articulation of known remaining risks, to support the DOI AO’s authorization to operate (ATO).
* **Continuous Monitoring Requirements.** DOI requires that the service provider comply with the continuous monitoring requirements consistent with applicable NIST standards. The service provider is required to share information in accordance with the continuous monitoring requirements defined for the applicable security controls. A Continuous Monitoring Plan (CMP) shall be developed by the service provider that focuses on specific requirements for monitoring the ongoing effectiveness of all applicable security controls (identified herein, in the *IT Security and Privacy Checklist (Appendix A)* and in the *DOI Security Control Standards)*, monitoring frequencies, and security status reporting frequencies and formats to the DOI Authorizing Official (AO), including all associated measures and metrics. (*DOI Security Control Standards* and in accordance with NIST SP 800-53A and NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*).

4. Personnel Security Background Investigations and Clearances

Acquired services shall comply with the following regulations and requirements. Homeland Security Presidential Directive-12 requires that all federal entities ensure that all contractors have current and approved security background investigations that are equivalent to investigations performed on federal employees. The Contractor shall comply with DOI policy relating to HSPD-12. Background investigations will be performed by the Office of Personnel Management (OPM) (See DIAPR 2010-04, Implementation of Homeland Security Presidential Directive-12 (HSPD-12) Part 2, DOI Access Program Implementation at <http://www.doi.gov/pam/DIAPR%202010-04.pdf>).

DOI separates the risk levels for personnel working on federal computer systems into three categories: Low Risk, Moderate Risk, and High Risk. The level/complexity of background investigations must be the same as for a Federal employee holding a similar position. Criteria for determining which risk level a particular contract employee falls into are shown in Illustration 1 of DOI’s Departmental Manual (DM) 441, Chapter 3 (available at: <http://elips.doi.gov/app_dm/act_getfiles.cfm?relnum=3860>). The DM Chapter provides guidance for the appropriate background investigations based on types of access. The Contractor shall ensure that only appropriately cleared personnel are assigned to positions that meet these criteria.

Those contract personnel determined to be in a:

* Low Risk position will require a National Agency Check with Written Inquiries (NACI) or equivalent investigation;
* Moderate Risk position will require either a Limited Background Investigation (LBI) or a Minimum Background Investigation (MBI) based on the Contracting Officer’s (CO) determination; and
* High Risk position will require a Background Investigation (BI).

The Contracting Officer, through the Contracting Officer’s Technical Representative or Program Manager will ensure that a completed Contractor Information Worksheet (CIW) for each Applicant is forwarded to the Federal Protective Service (FPS) in accordance with the DOI//FPS Contractor Suitability and Adjudication Program Implementation Plan dated 20 February 2007. FPS will then contact each Applicant with instructions for completing required forms and releases for the particular type of personnel investigation requested.

Applicants will not be reinvestigated if a prior favorable adjudication is on file with FPS or DOI, there has been no break in service, and the position is identified at the same or lower risk level.

After the required background investigations have been initiated, the Contractor may request authorization for employees whose investigations are pending to access systems supporting DOI

FCHS applications. The DOI Chief Information Officer may grant this authorization based on determination of risk to the government and operational need for the support of these applications.

Contractor shall comply and cause Provider to agree to comply with the United States Government and the DOI regulations as outlined in DM441, Chapter 3, in reference to background checks, position risk and sensitivity. The Provider is responsible for maintaining an up to date list of all personnel that have access to DOI data. This list shall be provided by the service provider at any time during the life of the contract when requested by the CO or COR via email. The vendor shall provide the list within three business days of the request.

5. Non-Disclosure Agreements (NDAs)

The Offeror shall require each employee that interfaces with the DOI cloud services data, its management, hosting, and delivery to sign non-disclosure agreements prior to beginning work on the DOI contract. Standard non-disclosure statements shall be provided as required for system administration personnel who may have access to government data in the course of their duties. NDAs typically utilized by the Offerer/Provider required to be signed by contractor staff may be utilized in lieu of the DOI standard NDAs provided they are deemed appropriate and acceptable by the Contracting Officer.

6.  Personnel Changes

The Provider shall notify the COR immediately when key employees having access to the FCHS system or DOI information are reassigned or leave the contractor’s employ, and prior to an unfriendly termination.

7. Government access

To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, confidentiality, integrity, availability, and reliability of any non-public government data collected and stored by the Offeror, the Offeror shall afford the government

access to the Offeror’s facilities, installations, technical capabilities, operations, documentation, records and databases. The Provider shall also identify how the following compliance, oversight and law enforcement objectives can be effectively and efficiently conducted by DOI in the event such activity is deemed by DOI to be appropriate and necessary relative to the facilities, installations, operations, documentation, databases, IT systems, devices, and personnel used in performance of the contract, regardless of the location:

* audits;
* inspections;
* evaluations;
* investigations;
* continuous monitoring of the security posture and continued effectiveness of management, operational and technical controls (including IT asset and device discovery, inventory and security configurations);
* penetration testing; and
* vulnerability testing.

The above are in addition to the similar types of activities outlined herein that are normally conducted by the Provider or independent assessors. Such activities are expected to occur only in rare instances where DOI determines that special circumstances necessitate additional measures to ensure the FCHS system is employing adequate safeguards against specific threats and hazards to the confidentiality, integrity and availability of DOI data/information or to the function of the FCHS system and the preservation of evidence of computer crimes.

The above objectives may be achieved by employing the services of mutually agreed to independent third-party auditors, inspectors, evaluators, investigators, or assessors as deemed appropriate by DOI. All associated information shall be available to DOI upon request.

8. Incident Detection, Notification, Handling, Response, Containment, Eradication, Recovery and Reporting

The Provider shall immediately report all incidents, whether suspected or confirmed, involving potential risks to the confidentiality, integrity or availability of DOI’s information or to the function of FCHS systems operated on behalf of DOI, to the DOI Computer Incident Response Center (DOI-CIRC), DOI Contracting Officer and DOI System Owner. The Provider shall report computer security incidents and breaches affecting DOI data/information or to the function of FCHS systems in accordance with the DOI Computer Incident Response Handbook. The Provider shall promptly coordinate with the DOI System Owner and DOI-CIRC on all related FCHS incident handling, response, containment, eradication, and recovery efforts throughout the incident lifecycle until fully resolved to the satisfaction of the DOI System Owner.

Upon becoming aware of any unlawful access to any DOI data/information stored on Provider’s equipment or in Provider’s facilities, or unauthorized access to such facilities or equipment resulting in loss, disclosure or alteration of any DOI data/information (a “Security Incident”), Provider will:

1. immediately notify the CO and COR’s via email with details of the Security Incident;
2. investigate the Security Incident and provide DOI with detailed information about the Security Incident; and
3. take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

If new or unanticipated threats or hazards are discovered by either the government or the Offeror, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.

9. Federal Information Security Management Act (FISMA)

At all times, the Contractor shall comply and the Contractor shall cause Provider to agree to comply with FISMA and OMB Circular A-130. This compliance shall include the completion and ongoing maintenance of the Assessment and Authorization (A&A – formerly referred to as Certification and Accreditation (C&A)) of the Provider service and adherence to DOI Policies on IT Security Management. The maintenance of the A&A is a requirement of the business relationship between DOI, the Contractor and Provider.

Continued utilization of the service by any DOI entity shall be dependent upon the completion and maintenance of the A&A.

The following NIST Federal Information Processing Standard Publications (FIPS Pubs) and Special Publications (SPs) are especially applicable to the Product Acquisition.  They are A&A focused. Successful completion of A&A includes, but is not limited to, these standards:

| **NIST Standards** |
| --- |
| FIPS Pub 199, *Standards for Security Categorization of Federal Information and Information Systems* |
| FIPS Pub 200, *Minimum Security Requirements for Federal Information and Information Systems* |
| SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories: (2 Volumes) - Volume 1: Guide Volume 2: Appendices* |
| SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View* |
| SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* |
| SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations* |
| SP 800-34, *Contingency Planning Guide for Federal Information Systems* |
| SP 800-30, *Guide for Conducting Risk Assessments* |
| SP 800-18, *Guide for Developing Security Plans for Federal Information Systems* |
| SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations* |
| SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans* |

Figure 1 – NIST A&A Related Standards

10. Assessment and Authorization (A&A)

The Offeror, using an independent assessor approved by the DOI Authorizing Official (AO), will perform the Assessment and Authorization (A&A – formerly referred to as Certification and Accreditation (C&A)) of the FCHS information system developed or maintained hereunder prior to going into production. Subsequent to the initial authorization to operate, required to be formally approved by the DOI AO, DOI requires that the FCHS information system follow the ongoing authorization process and associated continuous monitoring requirements as prescribed by OMB and NIST. This Provider shall assess the effectiveness of required implemented controls on an ongoing basis to inform the AO’s decisions regarding the continued use and operation of the system. A&A documents will be provided to the COR, DOI System Owner, and DOI AO in both hard copy and electronic forms.

The Contractor must obtain the appropriate A&A through validation of *security functionality* of required management, operational, and technical controls selected, documented in the System Security Plan (SSP), and formally approved by the DOI AO. The security control objectives for the FCHS IaaS, PaaS and SaaS information systems shall meet the overall security categorizations of “LOW”, “MODERATE” or “HIGH” commensurate with the DOI hosted applications, and corresponding individual potential risk impact ratings of “LOW”, “MODERATE” or “HIGH” for the Confidentiality, Integrity and Availability objectives and shall have selected and implemented appropriate security controls corresponding to those security categorizations (see NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, and 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*). Security functionality must be obtained by employing within the information system and its environment of operation, a combination of the appropriate set of management, operational, and technical security controls from NIST Special Publication 800-53 that correspond to the security categorization and associated potential risk impact ratings.

The Contractor must follow all relevant NIST FIPS Pubs and SPs to include, but not limited to, FIPS Pub 199 and 200, SP 800-39, 800-37, 800-137, 800-60, 800-53, 800-53A, 800-34, 800-30, and 800-18. The Contractor must also comply with all DOI IT security and Privacy policies and standards including, but not limited to, Departmental Manual (375DM19); DOI Security Control Standards (SCS), including the eighteen security control family standards; and the DOI Privacy Impact Assessment (PIA) requirements and associated templates.

Where the security control requirements outlined herein cannot be met, at the discretion of and approval by the DOI AO, either:

* other alternative mitigating/compensating controls can be offered by the Contractor for consideration and approval by the DOI AO;
* the DOI AO can formally document and accept the associated risk of not implementing a control or the residual risk level resulting from partial risk mitigation; or
* the DOI AO can reject risk acceptance and the proposed solution by not authorizing the system to operate.

Where a proposed FCHS information system provides for sufficient physical separation as a compensating/mitigating control obviating the need to impose one or more requirements outlined herein, the Contractor should provide the appropriate rationale and justification supporting such assertions for consideration, risk acceptance, and approval by the DOI AO.

The DOI AO for the FCHS information system is the Department’s Chief Information Officer (CIO).

The A&A on DOI systems to which the Contractor may have access under this contract will be conducted by the Government or another of its contractors.

11. Government support of the FISMA Assessment and Authorization (A&A) Process

The Government will timely review Provider’s Assessment and Authorization (A&A) documentation package and any changes submitted by Provider that could require re-assessment in order to assist the Government in its compliance with FISMA and the NIST 800-53 security control requirements. If there are any errors, omissions or other issues with the Provider’s A&A documentation package or assessment results, the Government will timely notify Provider and provide reasonable descriptions of specific errors, omission or other issues. The Government will reasonably cooperate with Provider in the A&A process and will not unreasonably withhold or delay any review of A&A package documentation, assessment result from the independent assessor, or authorization decisions.

Upon completion and acceptance of the A&A the Contractor is responsible for providing all signed documentation to the Contracting Officer and COR’s.

11.1 System Security Plan (SSP)

As part of the A&A, the Contractor shall develop a SSP in conformance with NIST SP 800-37, 800-39, 800-18, 800-60, 800-53, 800-137 and FIPS Pubs 199 and 200.

In addition to the NIST SP 800-53 minimum security control requirements applicable to the FCHS IaaS, PaaS and SaaS information system components having appropriate security controls selected and implemented for security categorizations of “LOW”, “MODERATE” or “HIGH” commensurate with the DOI hosted applications, the following additional requirements and enhancements apply:

**11.1.1 Auditable Events (AU-2) Control**

In addition to the types of events to be audited as specified by FedRAMP, the FCHS shall include automated auditing, alerting and reporting of all events in which any individual, other than the intended authorized individual(s), accesses any DOI information. Such events shall constitute a potential security violation, unless such access has been explicitly and formally approved by the DOI System Owner in writing, and reported to DOI as a potential incident in accordance with section 8 above (see *Incident Detection, Notification, Handling, Response, Containment, Eradication, Recovery and Reporting*).

**11.1.2 Maintenance Personnel (MA-5) Control**

Control Enhancements

1. The organization maintains procedures for the use of maintenance personnel that lack appropriate background investigations and security clearances or are not U.S. citizens, that include the following requirements:
   1. Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the information system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified;
   2. Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, all volatile information storage components within the information system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured; and
   3. In the event an information system component cannot be sanitized, the procedures contained in the security plan for the system are enforced.

Enhancement Supplemental Guidance: The intent of this control enhancement is to deny individuals who lack appropriate security clearances (i.e., individuals who do not possess security clearances or possess security clearances at a lower level than required) or who are not U.S. citizens, visual and electronic access to any Controlled Unclassified Information (CUI); information subject to the Privacy Act, including Personally Identifiable Information (PII); or any other sensitive agency information contained on the information system. Procedures for the use of maintenance personnel shall be documented in the security plan for the information system.

1. The organization ensures that personnel performing maintenance and diagnostic activities on an information system processing, storing, or transmitting sensitive agency information are cleared (i.e., possess appropriate background investigations and security clearances) for the highest level of information on the system.
2. The organization ensures that personnel performing maintenance and diagnostic activities on an information system processing, storing, or transmitting sensitive agency information are U.S. citizens.

11.2 Continuous Monitoring Plan (CMP)

The Provider shall submit a continuous monitoring plan that supports the DOI AO’s ongoing authorization process. The plan must conform to the NIST SP 800-137 and be formally approved by the DOI AO. The Contractor shall submit monthly continuous monitoring reports to the applicable Government System Owner and Authorizing Official.

The Contractor is required to conduct continuous monitoring of the FCHS information system in a manner that enables enterprise-wide visibility into the security posture and effectiveness of controls across the FCHS. The Contractor is required to monitor the security state of the FCHS information system on an ongoing basis with a frequency sufficient to enable the DOI AO to make ongoing risk-based decisions on whether to continue to utilize the system. The Contractor shall develop, document, and implement a continuous monitoring program for the FCHS information system and obtain approval of the continuous monitoring strategy by the DOI AO.

The continuous monitoring program must address, at a minimum: (i) the effectiveness of deployed security controls; (ii) changes to information systems and the environments in which the system operates; and (iii) compliance to federal legislation, directives, policies, standards, and guidance with regard to information security and risk management. In documenting the continuous monitoring program for the FCHS information system, the Contractor must identify and obtain approval by the DOI AO for the security controls to be monitored, the frequency of monitoring, and the control assessment approach. The program must define how changes to the FCHS information system will be monitored, how security impact analyses will be conducted, and the security status reporting requirements including recipients of the status reports.

The Contractor must apply the guidance provided in NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, and the supporting NIST SP 800-137, *Information System Continuous Monitoring for Federal Information Systems and Organizations*, in developing and implementing their continuous monitoring strategy for the FCHS information system. The Contractor shall take into consideration the criteria provided in the NIST standards in determining control assessment and monitoring frequencies. These criteria, as well as those provided in applicable OMB guidance for FISMA reporting (including associated Department of Homeland Security requirements for reporting of key metrics through submission of required data feed elements into CyberScope from automated security management tools), shall be used in determining the methodology for continuous monitoring supporting the ongoing system authorization process.

Information systems used or operated by Federal agencies, or by contractor(s) on their behalf, must be tested and evaluated annually. The security control assessment results may be drawn upon from the following sources to satisfy the annual FISMA requirement, including but not limited to:

* Security assessments conducted as part of an information system security authorization or re-authorization process;
* Continuous monitoring activities; or
* Testing and evaluation of the information system as part of the ongoing system development life cycle process (provided that testing and evaluation results are current and relevant to the determination of security control effectiveness).

Automated monthly discovery and reporting of all associated FCHS system physical and logical assets shall be conducted to maintain an accurate physical and logical inventory of all system components. Automated monthly vulnerability scans and verification of security configurations for all FCHS system physical and logical assets shall be conducted using authenticated and agent-based mechanisms to ensure the most comprehensive and accurate detection, identification and reporting of vulnerabilities and weaknesses in the FCHS information system and associated components. An electronic copy of each report and session data shall be provided to the COR and System Owner.

At least annually, the FCHS information system and associated components accessible from the Internet must be penetration tested by a mutually agreed to independent third-party assessor. Electronic and hard copy reports of penetration test results shall be provided to the COR and System Owner.

The Government reserves the right to conduct prearranged vulnerability scans or penetration tests using a mutually agreed to independent third-party assessor in accordance with a formally documented Memorandum of Agreement (MOA) and accompanying Rules of Engagement.

The Provider will take appropriate and timely action to correct or mitigate weaknesses discovered during such testing, at no additional cost.

The Contractor’s continuous monitoring program shall include providing, implementing, and maintaining all Security Content Automation Protocol (SCAP[[1]](#footnote-1)) compliant data feeds for all of the types of data elements (e.g., asset inventory and security configuration) required by the Department of Homeland Security (DHS) and upload them to the DHS CyberScope[[2]](#footnote-2) solution within the frequencies and formats established by DHS.

11.3 Contingency Plan (CP)

The Provider shall submit a contingency plan for restoration and testing of FCHS system services and resumption of maintenance support during a contingency operation. The plan must conform to the NIST SP 800-34 and be consistent with existing DOI continuity of operation procedures and plans. The Contractor shall submit contingency plans to the DOI System Owner.

11.4 Security Assessment Plan and Report (SAP/SAR)

The Offeror, using an independent third-party assessor approved by the DOI AO, will plan and conduct the security assessment of the FCHS information system in accordance with NIST SP 800-53A and document all identified vulnerabilities and weaknesses and appropriately characterize and assess the resulting risks in accordance with NIST SP 800-30 in the SAR.

The qualifications and required degree of independence of the assessors shall be at the discretion and approval of the DOI AO.

With the approval of the Government System Owner, and as required by the DOI AO, the Contractor will take immediate and timely action to correct or mitigate any vulnerabilities and weaknesses discovered, as necessary, to bring the application or system into compliance with the IT security and Privacy requirements outlined herein.

11.5 Plan of Action and Milestones (POA&M)

The Provider shall develop and maintain a POA&M documenting all known IT security vulnerabilities and weaknesses in the FCHS information system and associated components. The POA&M must contain the required elements identified in the DOI POA&M Processing Standard. The Contractor shall submit POA&Ms to the DOI System Owner and, in coordination with the DOI System Owner, provide quarterly briefings to the DOI AO regarding the corrective action status of known vulnerabilities and weaknesses and the risks they pose to DOI’s information and the FCHS information system.

11.6 Information Assurance (IA) Requirements

The Contractor services and associated solutions shall also implement the following requirements:

* Encryption of all sensitive data in transit (motion) and at rest (storage) using only NIST Validated FIPS 140-2 compliant and validated cryptographic modules and algorithms.
* Under some circumstances, the use of public or hybrid clouds and their associated risks may be deemed acceptable by the DOI Authorizing Official (AO) who shall make the risk-based determination in consultation with, and with the concurrence of, the Department’s Chief Information Officer (CIO). DOI is not aware of public or hybrid cloud solutions at this time that would meet the security requirements defined in this solicitation, federal policy, and individual task orders for “MODERATE” systems, but may become aware of these through the solicitation process or otherwise in the future. DOI does not wish to preclude potential interagency customers from implementing hosting in public or hybrid cloud solutions based upon their independent risk management processes, or to preclude hosting of DOI moderate systems in public or hybrid clouds if, and when, the specific security requirements defined in the RFP and the individual Task Orders can be met
* Access, transmit, process, house, and store all sensitive agency information, including information subject to the Privacy Act and Personally Identifiable Information (PII), only within the sole jurisdiction of the United States Federal Government (i.e., within the continental United States, Hawaii, Alaska, Puerto Rico, Guam, and the Virgin Islands).
* Conduct annual penetration testing using a qualified and competent independent third-party assessor/evaluator subject to approval by the DOI AO.
* Implement cloud service infrastructure and data storage redundancy in at least two facilities located within the sole jurisdiction of the United States Federal Government (i.e., within the continental United States, Hawaii, Alaska, Puerto Rico, Guam, and the Virgin Islands) with adequate geographical separation of at least 250 miles with one serving as the primary site and the other as an alternate backup Disaster Recovery (DR) site capable of restoration and resumption of FCHS services and complete preservation and reconstitution of all DOI data/information within 24 hours of failure of the services normally provided by the primary site.
* Seamlessly integrate with the DOI Identity, Authorization and Access Management (IdAAM) solution that consists of the Microsoft Active Directory (AD) and Public Key Infrastructure (PKI) architecture and associated Certificate Authority and DOI HSPD-12 PIV SmartCard-based credentials and enable logical authentication utilizing those credentials without requiring additional Contractor solution credentials; digital and electronic signing and signatures of emails and documents/content within the collaboration suite; and encryption of emails and documents/content using those capabilities.
* Provide a Data Loss Prevention (DLP) capability for the FCHS to detect and prevent the potential loss, exposure, or confidentiality risks to DOI’s sensitive agency information, including information subject to the Privacy Act and Personally Identifiable Information (PII), resulting from intentional or unintentional disclosure to external entities.
* The DLP capability shall be integrated in a manner that allows the agency to specify which recipient domains or individual entities are allowed (e.g., .GOV domains) to receive/access certain types of sensitive agency information (e.g., DOI business partners, and other external organizations whose security environments have been appropriately vetted and authorized to handle such information in a secure manner) and where such sensitive information is detected and domains or individual entities are approved that the content is encrypted by the application residing within the FCHS.
* Provide E-Discovery capabilities that enable compliance with legal mandates and requests capabilities to support legal hold requests.
* Provide solutions that conform to the Federal Desktop Core Configuration (FDCC) and United States Government Configuration Baseline (USGCB) security configuration requirements; and that are compatible with end-user client computing devices, operating systems, and client software/interfaces (e.g., workstations, laptops, mobile/portable devices) that are configured in accordance with those specifications; and that do not alter, or require alteration of, those baseline standard security configurations.
* Conform to, and implement the requirements of, the *Domain Name System (DNS) Security Reference Architecture*, Version 1.0 or later.

11.6.1 Cloud Service Delivery Model Security Requirements

The following General Requirements apply to all cloud service delivery models:

1. **Data Protection.** Obtain appropriate security assurance (see NIST SP 800-39) through an independent third-party assessor’s analysis of the provider’s data protection mechanisms, data location configuration and database organization/transaction processing technologies, and assess whether they will meet the confidentiality, compliance, integrity and availability needs of the agency.
2. **Multi-tenancy.** Under some circumstances, the use of public or hybrid clouds and their associated risks may be deemed acceptable by the DOI Authorizing Official (AO) who shall make the risk-based determination in consultation with, and with the concurrence of, the Department’s Chief Information Officer (CIO). DOI is not aware of public or hybrid cloud solutions at this time that would meet the DOI security requirements for “MODERATE” systems, but may become aware of these through the solicitation process or otherwise in the future. DOI does not wish to preclude potential interagency customers from implementing hosting in public or hybrid cloud solutions based upon their independent risk management processes, or to preclude hosting of DOI moderate systems in public or hybrid clouds if, and when, the specific security requirements defined in the RFP and the individual Task Orders can be met.
3. **Operating Policies.** Contractor shall:
4. submit to and fully cooperate with external audits, evaluations, assessments and security certifications to include, but not limited to, DOI approved and authorized IT security and Independent Verification and Validation (IV&V) staff employees or their designated support contractors, DOI Office of Inspector General (OIG), and the General Accountability Office (GAO);
5. establish incident response and recovery procedures and practices that integrate DOI Computer Incident Response Center (DOI-CIRC) and DOI Advanced Security Operations Center (ASOC) incident and breach detection, reporting, notification, handling, response, containment, eradication and recovery processes and that adequately inform DOI senior agency officials, AO, System Owner, and Information System Security Officer (ISSO) of incidents, remediation and containment actions, etc.
6. submit to and fully cooperate with internal investigation processes with respect to illegal or inappropriate usage of IT resources including, but not limited to, those investigations conducted by the Department’s Office of Human Resources for administrative investigations and those conducted by the OIG Computer Crimes Investigation Unit;

1. identify policies and procedures for vetting of privileged uses such as the provider’s system and network administrators that are deemed appropriate and acceptable to the DOI AO.
2. **Authentication.** Contractor shall support the enablement and use of strong authentication tokens in accordance with the Federal Identity, Credential, and Access Management (FICAM) implementation guidance, Homeland Security Presidential Directive (HSPD-12), and associated NIST standards and publications regarding use of the Personal Identity Verification (PIV) Smartcard logical authentication credentials for access to the cloud environment, software, applications, services or infrastructure by either provider or subscriber authorized system administrators and subscriber end-users in a manner that leverages DOI’s existing authentication infrastructure to mitigate the risk of account compromise or hijacking.
3. **Application Configuration.** Applications (including all associated IaaS, PaaS, and SaaS components shall be configured, as necessary, to run in a secure manner (e.g., a dedicated VLAN segment) and shall be integrated with existing enterprise/agency security frameworks (such as Identity, Authorization and Access Management (IdAAM) solution(s), Trusted Internet Connection (TIC) security infrastructure protection architecture, and Trusted Internet Connection Access Provider (TICAP) processes and procedures) such that enterprise/agency security policies are enforced through automated monitoring and detection. This includes ensuring, where necessary, all required components to route applicable and necessary application/network communications traffic through the DOI Trusted Internet Connection (TIC) gateways for monitoring and inspection consistent with DOI’s Trusted Internet Connection Access Provider (TICAP) and associated Advanced Security Operations Center (ASOC) security monitoring requirements, including any associated and/or required infrastructure security architecture protection systems, tools, and technologies in conformance with Office of Management and Budget (OMB) and Department of Homeland Security (DHS) TIC requirements and required capabilities.
4. **Secure Data Deletion and Disposition.** Contractor shall provide a mechanism for reliably deleting DOI data upon request by DOI as well as providing evidence that the data was deleted.
5. **Data Recovery.** The Contractor shall submit to, and fully cooperate with, DOI personnel to examine the capabilities of the provider with respect to:
6. data backup;
7. data archiving; and
8. data recovery.
9. **Physical.** The Contractor shall document and demonstrate adequate physical plant security practices and plans at provider sites that are deemed appropriate and acceptable to the DOI AO. Backup plans resulting from both physical and cyber attacks shall be incorporated into the overall plans. The Contractor shall offer redundancy for the sites they operate and provide sufficient geographic separation between alternate disaster recovery locations continued and/or reconstituted within mutually agreed upon timeframes established through Service Level Agreements (SLAs) in case of natural disasters or other disruptions.
10. **Acceptable Use Policies.** The Contractor shall not impose on DOI employees or contractors any additional requirements other than those articulated in DOI policies (e.g., IT Security, Privacy, Human Resources acceptable use policy, etc.) nor impose any penalties or sanctions on, or against, DOI employees for resolution of policy violations and accept that DOI’s handbook on Charges and Penalty Selection for Disciplinary and Adverse Actions, and associated Table of Penalties, are acceptable and to be applied at the management discretion of the agency.
11. **Licensing.** The Contractor shall properly license any proprietary software installed into their environment where DOI has a dependency on such software and associated functionality delivered by the provider as part of its service.
12. **Patch Management.** The Contractor shall document a set of procedures for DOI approval and agreement for what DOI needs to perform to take an application offline (whether a software patch is going to be installed by the provider or subscriber), the testing that must be performed to ensure the application continues to perform as intended, and the procedures needed to bring the application back online. Plans for system maintenance should be expressed in a Service Level Agreement (SLA).
13. **Legal.** Contractor shall offer capabilities to support ad hoc legal requests for:
    * + - 1. e-Discovery, such as litigation freezes, and
          2. preservation orders of data and meta-data.

For Software as a Service (SaaS) components, the Contractor shall demonstrate the following to the satisfaction and approval of the DOI AO.

1. **Client Device/Application Protection.** Consistent with the FIPS 199 security categorization and potential risk impact level of the data being processed (e.g., “LOW”, “MODERATE” or “HIGH” for each of DOI’s specific requirements commensurate with the security categorizations of DOI’s hosted applications), demonstrate to the independent third-party assessor that the cloud subscriber’s client devices (e.g., the agency’s client computers and mobile devices and associated client software that are necessary to interface with the FCHS) are adequately protected so as to control the exposure of the agency’s network and associated network resources and those of the FCHS to attacks.
2. **Encryption.** Strong encryption is required to be enforced by the SaaS application using a robust algorithm with keys of required strength in accordance with NIST FIPS Pub 140-2, *Security Requirements for Cryptographic Modules*, and NIST SP 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*, to be used for client sessions whenever the subscribed SaaS application requires the confidentiality of application interaction and data transfers. For Web sessions the Transport Layer Security Version 1.0 (TLS 1.0) protocol using the Advanced Encryption Standard (AES) 256 bit key cipher suite shall be enforced. The same diligence shall be applied to stored data using the AES 256 bit key cipher suite. All cryptographic algorithms and modules employed shall be only those approved for use by the Federal government and that have been tested, validated and approved by NIST through the Cryptographic Algorithm Validation Program (CAVP) and Cryptographic Module Validation Program (CMVP) and operating in a configuration mode that maintains the integrity of those protective measures.

For Infrastructure as a Service (IaaS) components, the Contractor shall demonstrate the following to the satisfaction and approval of the Authorizing Official (AO).

1. **Multi-tenancy.** When an IaaS cloud provider provides computing resources in the form of Virtual Machines (VMs), the provider shall have mechanisms in place to protect VMs from attacks
   * + - 1. from other VMs on the same physical host;
         2. from the physical host; as well as
         3. network originated attacks.

Typical attack detection and prevention mechanisms shall include Virtual Firewalls, Virtual IDS/IPS etc and network segmentation techniques such as VLANs.

1. **Administrative Access.** The IaaS cloud provider shall ensure that a limited set of DOI approved and authorized trained/trusted users (from the agency) alone are provided administrative access to any and all rented computing resources in the form of virtual machines or physical servers.
2. **VM Migration.** A documented strategy for future migration of Virtual Machines and their associated storage among alternate cloud providers shall be developed and maintained by the Contractor and approved by the agency (e.g., the OVF standard could be a partial basis for such a strategy).
3. **Virtualization Best Practices.** The Contractor shall follow best practices for the administration of conventional systems and networks, and for use of virtualization (i.e., NIST Guide to Security for Full Virtualization Technologies SP 800-125).
4. **Identity and Access Management.** The Contractor shall provide DOI visibility into to the following capabilities of the provider:
5. the authentication and access control mechanisms that the provider infrastructure supports;
6. the tools that are available for subscribers to provision authentication information; and
7. the tools to input and maintain authorizations for subscriber users without the intervention of the provider.
8. **Visibility.** The Contractor shall provide DOI visibility into the operating services that affect a specific agency subscriber’s data or operations on that data.
9. **Virtual Machines (VM) Vulnerabilities.** The Contractor’s computing resources offered in the form of VMs, shall include mechanisms provided by the provider to protect VM attacks from:
10. other VMs on the same physical host;
11. the physical host itself; and
12. network originated attacks.

Typical attack detection and prevention mechanisms include Virtual Firewalls, Virtual IDS/IPS, and network segmentation techniques such as VLANs.

VM image templates shall only be shared, made available for reuse, or implemented when designed from scratch and in a secure manner that prevents the possibility of any pre-existing authentication credentials or decryption keys from being inadvertently shared or used for unintended or unauthorized purposes.  VM image templates shall also be updated to incorporate the most current secure configurations and security patch levels as also required of VM production images already deployed and operating. These requirements are to address the risks inherent in trusting VM image templates to be free of backdoors, trojans, and other malicious code.

11.6.2 Independent Verification and Validation (IV&V)

In the development or maintenance of custom applications, software shall be independently verified and validated using a methodology determined appropriate by the DOI System Owner prior to being moved into production.

Contractor will ensure that IV&V, as deemed appropriate by the DOI System Owner, is performed on software deployed on Provider managed systems containing DOI data/information, in accordance with the methodology specified by the DOI System Owner.

11.6.3 Internet Logon Banner

A Government-approved logon banner must be displayed on the first page of any public access web pages.

11.6.4 Logon Warning Banner

Contractor employees who will access DOI data/information must acknowledge a Government-approved logon warning prior to each logon to the system.

11.6.5 Quality Control (Malicious Code)

All software and hardware shall be free of malicious code.

11.6.6 Security Controls

In the development or maintenance of custom applications, the Provider shall, with the knowledge and concurrence of the DOI System Owner, be responsible for IT security for all non-government-owned systems used in the development of, and systems intended for eventual delivery to, DOI in fulfillment of contract requirements. This includes IT, hardware, software, databases, networks, and telecommunications systems.

Security functionality in applications or integrated systems delivered hereunder must operate with the Government systems on, or with, which it will eventually be deployed. Products delivered hereunder must not cause misoperation of government resources or loss of confidentiality, integrity or availability of electronic information or data.

The Provider shall ensure compliance with the security control requirements of the current version of NIST FIPS Pub 200 and SP 800-53 and correspond to the information system potential risk impact ratings of “LOW”, “MODERATE” or “HIGH” for the Confidentiality, Integrity and Availability objectives, and overall “LOW”, “MODERATE” or “HIGH” information system security categorizations, commensurate with DOI’s hosted information and information systems and the associated FCHS IaaS, PaaS and SaaS information systems as DOI has determined based on FIPS Pub 199 and SP 800-60.

The Provider shall be responsible for IT security for all contractor-operated systems connected to a DOI network, regardless of location. The Contractor shall ensure compliance with the security control requirements of current version of NIST FIPS Pub 200 and SP 800-53 and appropriate to the sensitivity and criticality of the application/system.

11.6.7 Training

Provider employees must complete DOI’s end-user computer security awareness training, or equivalent, prior to being granted access to DOI data or being issued a user account. Training must be renewed annually. Provider employees are also required to annually complete IT security role-based training in accordance with the NIST SP 800-16, *Information Security Training Requirements: A Role- and Performance-Based Model*, and DOI’s Role-Based Security Training (RBST) Standard. The Provider shall annually prepare a report listing all Provider employees, security awareness course completion status by each employee, and IT security role-based training completion status by each employee with an explanation as to how each employee satisfied these annual training requirements. The Provider shall maintain records of all supporting evidentiary artifacts of completion and make them available for inspection/audit by the government upon request.

11.6.8 Privacy

11.6.8.1 Use of Personally Identifiable Information (PII)

The Contractor shall comply, and cause Provider to agree to at all times, with all requirements outlined herein to protect the Government’s information and data. Neither the Contractor nor Provider shall use any PII, Email Groups, Lists, or contact information for any purpose other than those activities necessary for the performance of this contract.

11.6.8.2 Transfer of Personally Identifiable Information (PII)

Personal information collected or otherwise processed by Contractor shall be accessed, transferred, stored or processed only within the sole jurisdiction of the United States Federal Government (i.e., within the continental United States, Hawaii, Alaska, Puerto Rico, Guam, and the Virgin Islands). The primary locations shall be the primary and back-up facilities located within the sole jurisdiction of the United States Federal Government (i.e., within the continental United States, Hawaii, Alaska, Puerto Rico, Guam, and the Virgin Islands). In addition, other sites include the location of teams who provide support to DOI in resolving issues regarding the email and collaboration solution, locations where backup or archiving facilities may be agreed to by DOI, or sites where antivirus and other security scans are performed. To the extent that material changes are made the Contractor shall use a mutually agreed upon Change Management Process to notify DOI.

12. Roles and Responsibilities

**12.1 Authorizing Official**

The authorizing official is the DOI Chief Information Officer (CIO). The DOI CIO formally assumes all risks to DOI for use of these external information services.

The authorizing official is responsible for:

* Reviewing and approving the security requirements, information security documentation, and CMP.
* Approving the authorization to operate (ATO).
* Reviewing risk reports on an ongoing basis.
* Disapproving the ATO if the trust relationship with the service provider is broken.

The authorizing official may rescind the authorization to operate immediately if an acceptable level of trust and applicable controls are not maintained, which may result in termination of the contract.

**12.2 Information Owner**

The information owner is the DOI official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information service. This is typically the management official who funds the acquisition for the system.

The information owner is responsible for:

* Ensuring a privacy impact assessment is performed.
* Ensuring a security categorization is performed.
* Ensuring the service provider assesses and implements all applicable controls.
* Ensuring that continuous monitoring is being performed.
* Reporting risk to the authorizing official as defined in the CMP.

Service Provider

The service provider is the third-party entity hired by the information owner to provide services external to the DOI network of services.

The service provider is responsible for:

* Collaborating with the information owner to implement all applicable controls.
* Performing continuous monitoring activities.
* Sharing information as required by the CMP.

13. IT Security Policies, Standards, Guidelines and Other Publications

One or more of the following sources of requirements relating to IT security and privacy have been incorporated by reference into the solicitation/statement of objectives. Copies of documents cited herein can be obtained as described below.

The following documents may be accessed electronically at these addresses:

* Office of Management and Budget (OMB) Circulars, Memoranda and Bulletins: <http://www.whitehouse.gov/omb/memoranda_default>
* National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) Publications and 800 Series Special Publications (SP): <http://csrc.nist.gov/publications/PubsSPs.html>;
* National Institute of Standards and Technology (NIST) Security Technical Implementation Guides (STIGs – also referred to as security configuration checklists): <http://web.nvd.nist.gov/view/ncp/repository>
* Federal Identity, Credential and Access Management (FICAM) Roadmap and Implementation Guidance: <http://www.idmanagement.gov/documents/FICAM_Roadmap_Implementation_Guidance.pdf>
* DOI Privacy Impact Assessment (PIA): <http://www.doi.gov/archive/ocio/privacy/pia.html>

Certain DOI documents are not publicly available. If one of these documents has been referenced elsewhere in this solicitation, it will be provided to interested Offerors under an appropriate non-disclosure agreement (NDA) upon receipt by the Contracting Officer of a written request signed by a responsible official of that organization.

[THE REMAINDER OF THIS PAGE INTENTIONALLY LEFT BLANK]

# APPENDIX A

# IT Security and Privacy Checklist

For External Information System Services

Step 1: Privacy Impact Assessment (DOI Responsibility)

The information owner is required to complete a Privacy Impact Assessment to identify if there is any Personally Identifiable Information (PII) being generated, stored, processed, or exchanged by the system.

Step 2: Security Categorization (DOI Responsibility)

The information owner is required to categorize the system and the information processed, stored, or transmitted by the system in accordance with FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, and document the results (including supporting rationale) in the system security plan.

Step 3: Information Security Documentation (DOI & Service Provider Responsibility)

The service provider is required to develop and maintain system security documentation that reflects the current security posture of the information system. The information security documentation and the required content are determined by NIST standards and *DOI Security Control Standards*.

Step 4: Security Assessment (DOI & Service Provider Responsibility)

The service provider is required to perform a security assessment, using a trusted independent assessor, by assessing the controls identified in the *DOI Security Control Standards* and ensuring the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting security requirements.

Step 5: Authorization to Operate (DOI & Service Provider Responsibility)

The DOI Authorizing Official must approve the ATO. The ATO is a formal declaration by the authorizing official that an information service is approved to operate in a particular security mode, using a prescribed set of safeguards and at an acceptable level of risk.

Step 6: Continuous Monitoring (DOI & Service Provider Responsibility)

The information owner and service provider are required to maintain the security level of the system over time by implementing and monitoring the security controls identified in the *DOI Security Control Standards,* and the supporting CMP,on an ongoing basis.

# APPENDIX B

# Deliverable and Reporting Requirements

**Deliverables and Reports:**

| **Title** | **Description** | **Due Date/Frequency** | **Government Approval and Surveillance** |
| --- | --- | --- | --- |
| Information Assurance (IA) Documentation | As described in, and in accordance with, the FCHS IT Security and Privacy Requirements document. | Upon Completion prior to authorization to move to Service Ready status | Contracting Officer’s Representative (COR), Government system owner, Government Authorizing Official (AO) (COR) |
| System Security Plan (SSP) | As described in, and in accordance with, the FCHS IT Security and Privacy Requirements document.. | Upon Completion prior to authorization to move to Service Ready status | Contracting Officer’s Representative (COR), Government system owner, Government Authorizing Official (AO) |
| Continuous Monitoring Plan (CMP) | As described in, and in accordance with, the FCHS IT Security and Privacy Requirements document. | Upon Completion prior to authorization to move to Service Ready status | Contracting Officer’s Representative (COR), Government system owner, Government Authorizing Official (AO) |
| Preliminary Privacy Impact Analysis (PIA - Privacy Threshold Analysis (PTA)) | As described in, and in accordance with, the FCHS IT Security and Privacy Requirements document. | Upon Completion prior to authorization to move to Service Ready status | Contracting Officer’s Representative (COR), Government system owner, Government Authorizing Official (AO) |
| Privacy Impact Analysis (PIA) | As described in, and in accordance with, the FCHS IT Security and Privacy Requirements document. | Upon Completion prior to authorization to move to Service Ready status | Contracting Officer’s Representative (COR), Government system owner, Government Authorizing Official (AO) |
| Contingency Plan | As described in, and in accordance with, the FCHS IT Security and Privacy Requirements document. | Upon Completion prior to authorization to move to Service Ready status | Contracting Officer’s Representative (COR), Government system owner, Government Authorizing Official (AO) |
| Independent Assessor’s Security Assessment Plan and Report (SAP/SAR) | As described in, and in accordance with, the FCHS IT Security and Privacy Requirements document. | Upon Completion prior to authorization to move to Service Ready status | Contracting Officer’s Representative (COR), Government system owner, Government Authorizing Official (AO) |
| Plan of Action and Milestones (POA&M) | As described in, and in accordance with, the FCHS IT Security and Privacy Requirements document. | Upon Completion prior to authorization to move to Service Ready status and Quarterly Thereafter | Contracting Officer’s Representative (COR), Government system owner, Government Authorizing Official (AO) |
| Vulnerability and Security Configuration Scan Report | As described in, and in accordance with, the FCHS IT Security and Privacy Requirements document. | Monthly | Contracting Officer’s Representative (COR), Government system owner |
| Continuous Monitoring Report | As described in, and in accordance with, the FCHS IT Security and Privacy Requirements document. | Monthly | Contracting Officer’s Representative (COR), Government system owner, Government Authorizing Official (AO) |
| Independent Penetration Testing and Report | As described in, and in accordance with, the FCHS IT Security and Privacy Requirements document. | Annually | Contracting Officer’s Representative (COR), Government system owner, Government Authorizing Official (AO) |
| Documentation for Audit Requirements | As described in, and in accordance with, the FCHS IT Security and Privacy Requirements document. | 30 calendar days after written request | Contracting Officer’s Representative (COR), Government system owner, Government Authorizing Official (AO) |
| Training Compliance Report | As described in, and in accordance with, theFC IT Security and Privacy Requirements document. | Annually | Contracting Officer’s Representative (COR), Government system owner |
| Security Incidents | As described in, and in accordance with, the FCHS IT Security and Privacy Requirements document. | Per Incident (immediately but not more than 2 hours) | Contracting Officer (CO), Contracting Officer’s Representative (COR), Government system owner, Government Authorizing Official (AO), DOI-CIRC |
| Contractor Employee Report | Report of all contractor employees that have access to DOI Data with status of required background checks as specified. | Annually on contract award anniversary date and within 3 business days upon written request | Contracting Officer’s Representative (COR) |

1. See <http://scap.nist.gov/> [↑](#footnote-ref-1)
2. See <http://scap.nist.gov/use-case/cyberscope/> [↑](#footnote-ref-2)