General Services Administration

Office of Professional Services and Human Capital Categories (PSHC)
Office of Contract Operations (QRAD)
for the
GSA Center for Charge Card Management (CCCM)

Statement of Objectives for GSA SmartPay® Agile Development Services

1.0 Background and Purpose

The GSA Center for Charge Card Management (hereinafter "CCCM") administers the GSA SmartPay Program, which is the world's largest government charge card and commercial payment solutions program. Providing services to nearly 600 federal government agencies, organizations, and Native American tribal governments, GSA SmartPay payment solutions enable authorized government employees to make purchases to support agency and organization missions.

1.1 Purpose

This program has interfaced and provided support to users through: (1) GSA SmartPay main website, and (2) GSA SmartPay training website.

1.1.1 Current state

(1) The GSA SmartPay main website is available at https://smartpay.gsa.gov and is:
- Built on a Drupal version 9 with PHP programming.
- Hosted on Red Hat Enterprise Linux version 8 servers.

The website received more than 1.8 million visitors (mobile & web) in FY22. Based on current content and development in progress, the government anticipates that traffic will be driven by state sales tax content and visits to the Section 889 Representations tool.

Section 889 of the 2019 National Defense Authorization Act prohibits purchases from certain banned telecommunication and video surveillance equipment in an effort to protect national security. The Section 889 Representations tool searches for company 889 status with Unique Entity Identifier (UEI), company name, or Commercial and Government Entity code (CAGE) number via the SAM.gov Entity Management application programming interface (API). The current 889 Representation tool is:

- Built on GSA's instance of Google Cloud Platform.
- Developed with Python (back-end) and Vue.js (front-end).

(2) The GSA SmartPay training website, which is available at https://training.smartpay.gsa.gov, provides mandatory training to card/account holders, approving officials (AOs), and agency/organization program coordinators (A/OPCs), as required by law and policy. This offering is optional for agencies to use

(some prefer to host their own content in their learning management systems). The current GSA SmartPay training website:

- Is built on a Drupal version 9 with PHP programming.
- Is hosted on Red Hat Enterprise Linux version 8 servers.
- Uses a MariaDM database.
- Has five on-demand, HTML-based training courses, which include:
    - Purchase Training for Card/Account Holders/AOs
    - Travel Training for Card/Account Holders/AOs
    - Purchase Training for A/OPCs
    - Travel Training for A/OPCs
    - Fleet Training for A/OPCs

Certificates are issued after the completion of a multiple question quiz with a passing score of 75%. There are approximately 700,000 current accounts and just under 600,000 visitors in FY22.

All information posted on the GSA SmartPay main website and GSA SmartPay training website is public. The government owns all code, data, image licenses, user information, and domain names.

1.1.2 Minimally Viable Products

Currently, CCCM program has partnered with the GSA Service Delivery team to build a minimally viable product (MVP) of the main website and training website using an iterative and user-centered delivery cadence. The Service Delivery team expects the MVP for each website to be delivered by summer 2023 and will work with the Contractor to transition the project.

The new GSA SmartPay main website (GitHub) will:

- Be hosted on Cloud.gov Pages (formerly known as Federalist).
- Leverage the static site generator, Eleventy.
- Incorporate the U.S. Web Design System.

The above-mentioned 889 tool will be migrated from Google Cloud Platform to Cloud.gov and Cloud.gov Pages before launch of the new GSA SmartPay main website.

The new GSA SmartPay training website (GitHub) will be a combination of static web content and a custom training application with a database component. The training website will be hosted on Cloud.gov and Cloud.gov Pages.

1.1.3 Future state

CCCM is seeking a Contractor to take the MVP of each website and continue future development. The Contractor will continue to build off the open source code developed by the Service Delivery team and develop enhanced functionality based on user needs, programmatic needs, and changes in policy. The Contractor will need to continue to add content and functionality using GitHub and support CCCM's ability to update content using front-end tools, such as Decap content management system (formerly known as Netflify).

The Service Delivery team is available to support transition.

Implementation and documentation is ongoing — current specifications are published to the Github repos. These repositories include supplementary information to this RFQ (see also Wikis found here and here).

1.2 Problems

The current GSA SmartPay main website is difficult for users to navigate intuitively. CCCM has challenges keeping content current and ensuring content is accessible to all audiences.

The current GSA SmartPay training website suffers from performance issues, which cause users to time-out in the middle of quizzes or experience random crashes. Since users login so infrequently, they often forget their passwords and need manual assistance in some cases to reset passwords which is a drain on CCCM resources. Reporting is limited and only available at the agency level; for large agencies, this is too untenable to track, and they're requiring users to email agency coordinators their certificates to manually check them off a list.

2.0 Scope

CCCM seeks agile software development services. The services to be provided will include all aspects of the software development process, including planning, design, software development and coding, prototyping, documentation, and testing. The services also include support of GSA security documentation and testing.

CCCM intends that the software delivered under this task order will be committed to the public domain. The Contractor will have to obtain CCCM's permission before delivering software under this task order that incorporates any software that is not free

and open source. The Contractor must post all developed code to a GitHub repository designated by CCCM.

2.1 Product Vision

Make it easier for SmartPay stakeholders to find the information they're interested in, and for the SmartPay PMO to keep the website updated and accessible to users.

2.2 Anticipated Period of Performance, Budget, and Ceiling Price

The period of performance (PoP) shall be one year, with options to extend up to two additional years. GSA may, by written notice issue and at least 60 days prior to the expiration of the initial term, extend the period of performance for additional option years in accordance with FAR Subpart 52.217-9 Option to Extend the Term of the Contract. The PoP is expected to begin on or around Aug 1, 2023.

The not to exceed ceiling on this contract will be $840,000 for the first period of performance (52.232-22 Limitation of Funds applicable) and up to an additional $550,000 for each of the two option periods. Contractors are expected to submit a quote reflective of its solution to fulfill the government's requirements.

The government may require continued performance of any services within the limits and at the rates specified in the task order in accordance with FAR Subpart 52.217-8 - Option To Extend Services, evaluation will be accomplished by using the prices offered for the last option period to determine the price for a 6-month option period, which will be added to the base and other option years to arrive at the total price. Evaluation of options will not obligate the Government to exercise the option(s).

3.0 Objectives

3.1 Backlog

The set of preliminary user stories set forth below will be the starting point for the development of software to be provided by the Contractor under this task order. These preliminary user stories are provided only for illustrative purposes, and do not comprise the full scope or detail of the project. CCCM expects that the Contractor will work closely with CCCM Product Owner(s) to develop and prioritize a full gamut of user stories as the project progresses.

Individual user stories may be modified, added, retracted, or reprioritized by CCCM at any time, and CCCM expects that the user stories will be continuously refined during the development process.

Programmatic data

- As an Agency / Organization Program Coordinator (A/OPC), I want information relevant for agency spend, so I can provide this to agency Chief Financial Officers as requested.
- As an A/OPC, I want access to travel spend by region, so I can understand regional spend trends for travel.

Training reporting

- As an A/OPC, I want users to be sent automatic reminders for training, so that certification requirements are automatically managed by the training platform.
- As a Level 1 A/OPC, I want to have reports automatically sent to me at indicated time frames, so I can have regular access to reports without having to access the system.
- As an A/OPC and administrator, I want to have customizable reports, so I have the ability to further analyze data.

Administrative functions

- As a system administrator, I want to perform periodic database purges for users who exist in the system but have not completed any quizzes so I can keep the database up-to-date and reduce storage requirements.
- As a system administrator, I want to be able to post system messages, so I can alert users to website status.
- As a system administrator, I want a user friendly maintenance interface, so I can easily make content changes.
- As a system administrator I want to be able to modify a user's profile in the database, so that I can correct incorrect or out-of-date information.

Email usage/monitoring

- As a system administrator, I want to be able to confirm what emails were sent to whom and when, so that we can ensure users are being properly notified.
- As a system administrator, I want to monitor email bouncebacks, so that I can take corrective action (as needed) to ensure users are being properly notified.

- As a system administrator, in the event of important information / notification, I need the ability to send emails to all users.

Other

- As an A/OPC and card holder, I want access to interactive content, so I can engage with the content in the forum I feel most comfortable.
- As an A/OPC and card holder, I want quick access to GSA SmartPay's social media accounts, so that I can stay apprised of program information / announcements.
- As the GSA SmartPay program, we want to implement GSA's instance of Google Tag Manager, in order to have more transparency into how our users are using our main website and training website.

Security

- As the system administrator, I need [a specific system vulnerability] that was discovered during penetration testing to be remediated, to ensure the training website remains secure.
- As the system administrator, I need [a specific item] to be updated, to comply with updated GSA IT security policies, standards and guidelines.
- As a system administrator, I need to remediate vulnerabilities based on authenticated scans, to comply with monthly security deliverable requirements.
- As a system administrator, I need the System Security Plan to be updated, to reflect a significant change in the system.

3.2 List of Deliverables with Quality Assurance Surveillance Plan (QASP)

The following chart sets forth the performance standards and quality levels the code and documentation provided by the Contractor must meet, and the methods CCCM will use to assess the standard and quality levels of that code and documentation.

Deliverable	Performance Standard(s)	Acceptable Quality Level	Method of Assessment

Tested Code	Code delivered under the order must have substantial test code coverage	Minimum of 90% test coverage of all code. All areas of code are meaningfully tested	Combination of manual review and automated testing
Properly Styled Code	18F Coding Styles Reference Guide	0 linting errors and 0 warnings	Combination of manual review and automated testing
Accessible	Web Content Accessibility Guidelines 2.1 AA standards	0 errors reported using an automated scanner and 0 errors reported in manual testing	Combination of manual review and automated testing (such as pa11y)
Deployed	Code must successfully build and deploy into staging environment	Successful build with a single command	Combination of manual review and automated testing

Documented	Summary of user stories completed every sprint. All dependencies are listed and the licenses are documented. Major functionality in the software/source code is documented. Individual methods are documented inline in a format that permits the use of tools such as JSDoc. System diagram is provided. Relevant security controls are documented and kept up to date.	Combination of manual review and automated testing, if available	Manual review

Secure	Code is free of known static and runtime vulnerabilities	Code submitted must be free of medium- and high-level static and dynamic security vulnerabilities	Tests free of medium- and high-level vulnerabilities from a static testing SaaS (such as Snyk or npm audit), from dynamic testing tools like OWASP ZAP (with documentation explaining any false positives), and ongoing code review informed by OWASP or similar standards

4.0 Contract Place of Performance and Contract Type

The Contractor may choose the location(s) from which to perform the required software development services so long as the work is performed in the Contiguous United States (CONUS). CONUS is defined as the 48 contiguous States and the District of Columbia. CCCM's core customer service hours are 8:00 am - 4:00 pm ET; we expect the software development team would be available 11:00 am - 4:00 pm ET, but we would need an assigned point of contact outside those hours if urgent matters arise.

CCCM intends to issue a time and materials task order under an existing contract under the Multiple Award Schedule ("Schedules") Technology's Special Item Number (SIN) 54151S for IT Professional Services, and all quotes must be submitted on that basis. CCCM will not consider quotes that include fees for licenses or subscriptions.

5.0 Operating Constraints (Non-functional Requirements)

5.1 Environment

- Software development services will occur in the GSA SmartPay Github environment(s).
- Website usage will be tracked with the Digital Analytics Program.
- Hosting will be on Cloud.gov Pages for building and serving front-end static assets and Cloud.gov for serving APIs and hosting the database and other backend services. Services are provided through an interagency agreement that CCCM has in place with Cloud.gov.
- Current coding languages are Python for the back-end and JavaScript (Astro and Vue.js) for the front-end. The government is not prescribing that these must be the coding language(s) moving forward.

5.2 Design

- Software development services shall leverage the U.S. Web Design System.
- Content development will follow CCCM style guide.

5.3 System Access

- All Contractor personnel working under the task order will need to be U.S. citizens.

- Homeland Security Presidential Directive 12 (HSPD-12) applies to Contractor development personnel as such performance requires access to internal Government information technology (IT) systems. As a result of HSPD-12 applicability to the requirements of this document, the Government will perform all required background investigations for Contractor personnel, and the Contractor shall ensure their personnel requiring physical access to Federally-controlled information technology systems have identification that complies with HSPD-12 policy. Immediately upon award the credential process shall commence. All identified Contractor personnel must complete a GSA Form 850 – Contractor Information Worksheet (CIW) to be provided with the quote submission. The Contractor will not be given the Notice to Proceed (NTP) to start work until all Contractor personnel have the proper identification to satisfy this requirement.
- Medium risk security clearance (Tier 2) shall be required.The Contractor will be responsible for the cost associated with the background investigation and clearance.
- NIST phishing resistant multi-factor authentication (MFA) shall be required for privileged and non-privileged users where login is required.

5.4 Security

The Contractor shall comply with the technology security requirements in the Federal Information Security Management Act (FISMA) (44 .S.C. 3544); the applicable National Institute of Standards and Technology; GSA IT security policies, standards and guidelines; and other Government-wide laws and regulations for protection and security of IT. The required policies and regulations are specified in Security and Privacy Requirements for IT Acquisition Efforts CIO-IT Security-09-48 (Attachment A) or latest version and Managing Enterprise Cybersecurity Risk CIO-IT Security-06-30 or latest version (Attachment B).

Security compliance will be continuous through DevSecOps practices and via user stories issued in sprint planning. Additional information about security and confidentiality requirements can be found in the current version of CIO_21001N_GSA_Information_Technology_Security_Policy (Attachment C).

5.4.1 Specific Security Requirements

The Contractor shall have all staff members complete a confidentiality agreement prior to starting contract performance.

5.5 Personnel Skills and Knowledge

Key Personnel – The Contractor must designate both a Project Manager (PM) and a Technical Lead (or labor category equivalent) as Key Personnel for this project. The PM will be a direct liaison to the CCCM product team, and will be responsible for the supervision and management of all of the Contractor's personnel. The Technical Lead must have a full understanding of the technical approach to be used by the Contractor's development team and will be responsible for ensuring that the Contractor's development team follows that approach.

Key Personnel Substitution – Key Personnel substitutions must be approved by CCCM in writing. Contractor requests for a substitution of Key Personnel must include a detailed explanation of the justifying circumstances, and a complete résumé for the proposed substitute or addition, including skills, experience, education, training, and security level.

Teaming Arrangements – No teaming will be permitted.

5.6 Special Clauses

Data Rights and Ownership of Deliverables – CCCM intends that all software and documentation delivered by the Contractor will be owned by CCCM and committed to the public domain. This software and documentation includes, but is not limited to, data, documents, graphics, code, plans, reports, schedules, schemas, metadata, architecture designs, and the like; all new open source software created by the Contractor and forks or branches of current open source software where the Contractor has made a modification; and all new tooling, scripting configuration management, infrastructure as code, or any other final changes or edits to successfully deploy or operate the software.

To the extent that the Contractor seeks to incorporate any software that was not first produced in the performance of this task order in the software delivered under this task order, CCCM encourages the Contractor to incorporate either software that is in the public domain, or free and open source software that qualifies under the Open Source Definition promulgated by the Open Source Initiative. The Contractor must obtain written permission from CCCM before incorporating into the delivered software any software that is subject to a license that does not qualify under the Open Source Definition promulgated by the Open Source Initiative. If CCCM grants such written

permission, then the Contractor's rights to use that software must be promptly assigned to CCCM.

If software delivered by the Contractor incorporates software that is subject to an open source license that provides implementation guidance, then the Contractor must ensure compliance with that guidance. If software delivered by the Contractor incorporates software that is subject to an open source license that does not provide implementation guidance, then the Contractor must attach or include the terms of the license within the work itself, such as in code comments at the beginning of a file, or in a license file within a software repository.

5.7 Invoicing/Payment

5.7.1 Invoices

In addition to the requirements defined in sections 5.7.3 and 5.7.4 below, to constitute a proper invoice, the billing document must include the following information and/or attached documentation:

(1) Name of Contractor and Contractor's Taxpayer Identification Number;

(2) Period covered by invoice and invoice date;

(3) Purchase order number;

(4) All invoices for services must set forth in detail the following:

  (i) Individual performing service each day by hour and quarter of an hour;

  (ii) Type of services performed each day by hour and quarter of an hour; and

  (iii) Hourly rate for each service so detailed;

(5) Any applicable payment discount terms; and

(6) Total amount billed.

5.7.2 Procedures for Payment

The government intends to make payment to the Contractor via charge card as outlined in accordance with (IAW) FAR 52.232-36, Payment by Third Party. Pursuant to IAW FAR 32.1108(b)(2)(ii), the contracting officer shall not authorize the Governmentwide commercial purchase card as a method of payment during any period the System for Award Management (SAM) indicates that the Contractor has delinquent debt subject to collection under the Treasury Offset Program (TOP). In such

cases, payments under the contract shall be made in accordance with the clause at 52.232-33, Payment by Electronic Funds Transfer-System for Award Management, or 52.232-34, Payment by Electronic Funds Transfer-Other Than System for Award Management, as appropriate (see FAR 32.1110(d)).

5.7.3 Payment by Governmentwide commercial purchase card

The Contractor shall submit invoices not more frequently than once per month. Payment shall be made in accordance with the clause found at FAR 52.232-36, Payment by Third Party. The Contractor shall make payment requests through a charge to the Government account with the third party, at the time and for the amount due in accordance with those clauses of this contract that authorize the Contractor to submit invoices, contract financing requests, other payment requests, or as provided in other clauses providing for payment to the Contractor.

On each invoice, the Contractor shall provide a summary of each billed CLIN. The summary shall include by each invoiced CLIN: CLIN number and description, as well as the invoiced amount. The invoice shall also provide a total amount, across all CLINs, billed to date. The Contractor shall not bill, nor be reimbursed, for any charges that are not specifically stated in this task order or incorporated via a written modification issued by the CO.

Please note, the payment via purchase card is rescinded should the Contractor's System for Award Management (SAM) registration indicate that the Contractor has delinquent debt that is subject to collection under the Treasury Offset Program (TOP).

5.7.4 Electronic Funds Transfer Method

The Contractor shall submit invoices not more frequently than once per month. Payment shall be made in accordance with the clause found at FAR 52.212-4 Contract Terms and Conditions – Commercial Items (Nov 2021), paragraph(g), following receipt of properly executed invoices prepared in accordance with the requirements of this task order.

On each invoice, the Contractor shall provide a summary of each billed CLIN. The summary shall include by each invoiced CLIN: CLIN number and description, as well as the invoiced amount. The invoice shall also provide a total amount, across all CLINs, billed to date. The Contractor shall not bill, nor be reimbursed, for any charges that are not specifically stated in this task order or incorporated via a written modification issued by the CO.

The Contractor has the option to submit an electronic or hard copy original invoice for payment to GSA Financial Information & Operations Division.

Electronic Invoices are encouraged and may be submitted to the following address: https://vcss.ocfo.gsa.gov

Invoices may also be submitted in lieu of electronic submission to:

USDA-OCFO
Financial Information & Operations Division
Financial Operations & Disbursement Branch
2300 Main Street – 2SE
Kansas City, MO 64108
Tel: (800) 676-3690/(816) 926-7287
Fax: (816) 926-5189

A duplicate electronic invoice with supporting documentation shall be sent electronically to the COR and CO. The COR will confirm performance made against the invoiced line items to ensure that the correct amounts have been billed and will document any price deductions. The COR will then certify and provide a signature indicating that the invoice is valid for payment. Invoices are authorized for payment upon the Government's receipt and acceptance of deliverables specified in the task order and the receipt of a valid invoice. Invoices shall be rendered no later than the 15th calendar day of the month following performance and must be accompanied by all status reports submitted during that period. The COR must receive a copy of the invoice and all supporting documentation (i.e. list of daily hours worked by each of the vendor's employees (also summed up as weekly and monthly for each person)) before or at the same time as the GSA Finance Office. All final invoices must be submitted no later than thirty (30) calendar days after the last day of the month for which the charges, either labor and/or ODCs, were incurred. The Contractor may invoice only for hours, travel, and/or unique services ordered by GSA and actually used in direct support of the program office for this task order.

Invoices must include the following:

(1) Name and address of the Contractor

(2) Invoice date and number

(3) GSA Multiple Award Schedule (MAS) Information Technology Professional Services Contract Number, line item number and, if applicable, the order number

(4) Description, quantity, unit of measure, unit price and extended price of the items delivered

(5) Shipping number and date of shipment, including the bill of lading number and weight of shipment if shipped on a Government bill of lading

(6) Terms of any discount for prompt payment offered

(7) Name and address of official to whom payment is to be sent

(8) Name, title, and phone number of person to notify in event of defective invoice

(9) Taxpayer Identification Number (TIN). The Contractor shall include its TIN on the invoice only if required elsewhere in this contract

(10) Electronic funds transfer (EFT) banking information

Note: Failure to comply with the procedures outlined above may result in the invoice being rejected, or your payment being delayed.

5.8 Limitation of Funds

The Contractor shall notify the CO in writing when it has reason to believe that the costs it expects to incur under this contract in the next 60 days, when added to all costs previously incurred, will exceed 75 percent of (1) the total amount so far allotted to the contract by the government. The notice shall state the estimated amount of additional funds required to continue performance for the period specified in the contract.

Sixty days before the end of the period specified in the contract, the Contractor shall notify the CO in writing of the estimated amount of additional funds, if any, required to continue timely performance under the contract or for any further period specified in the contract or otherwise agreed upon, and when the funds will be required.

6.0 Instructions and Evaluation

6.1 Submission Instructions

6.1.1 Before submitting a quote - Questions and Answers

Questions

Submit all questions concerning this RFQ through this Google form [link will be included in the final RFQ]. All questions must be submitted by [date will be provided in the final RFQ].

Questions should clearly express the Contractor's issues or concerns and must follow the format provided in the Google form. Statements expressing opinions, sentiments, or conjectures are not considered valid inquiries and will not receive a response. Further, Contractors are reminded that the government will not address hypothetical questions aimed at receiving a potential "evaluation" decision.

Answers will be provided as an amendment to the solicitation three business days after the deadline for questions.

6.1.2 Submission checklist

All responses must be submitted using this Google form and include the following materials:

Technical Submission:

- ☐ Technical approach - **4 pages** maximum, including diagrams, 12-point font
- ☐ Maximum of 2 code repositories with a short description about the project for each code repository
- ☐ Staffing plan - **3 pages** maximum, including diagrams, 12-point font
- ☐ Resumes and letters of intent from designated key personnel (if not currently employed by Contractor)
- ☐ User research plan
- ☐ Conflict of Interest (form to sign)
- ☐ FAR 52.204-24 Provision (checkbox on Google form)

Price:

Price responses must be submitted using the google form [will be provided with the final RFQ] and include the following materials:

- ☐ Price Quote (spreadsheet)

Interviews:

The government reserves the right to hold oral interviews. If the decision is made to hold interviews, Contractors will be notified and held in accordance with “Interviews” under **6.2 Instructions for Quotes** The oral interview does not require Contractors to submit any materials.

Applies to all phases: **Only submit information explicitly requested in this RFQ**. Do not include assumptions, caveats, or exceptions in any part of your submission. Failing to follow these instructions may result in removal from consideration for the award.

6.2 Instructions for Quotes

6.2.1 Technical Submissions

Technical submissions must consist of a technical quote of no more than four (4) pages, a staffing plan of no more than three (3) pages plus resumes and signed letters of intent to participate, and references to two source code samples, preferably open source. Technical quotes and staffing plans must be submitted using 12-point font.

The technical quote must set forth the Contractor's proposed approach to providing the services required, including programming language(s) the Contractor proposes to use. The technical quote must also make clear that the Contractor understands the details of the project requirements. The technical quotemust also identify potential obstacles to efficient development and include plans to overcome those potential obstacles.

The staffing plan must set forth the Contractor's proposed approach to staffing the requirements of this project, including the titles of each of the labor categories proposed and proposed level of effort for each member of the Contractor's development team. The staffing plan must also identify the proposed Project Manager and proposed Technical Lead by name, and include a resume for each. Those resumes

must include a brief description of the experience and capability for each individual, but cannot exceed one (1) page in length each. Contractors proposing Key Personnel who are not currently employed by the Contractor must include a signed letter of intent from the individual proposed as Key Personnel that they intend to participate in this project for at least one (1) year. The staffing plan must also set forth the extent to which the proposed team for this project was involved in the development of the source code referred to below.

The staffing plan must set forth and explain the extent to which the Contractor will provide individuals with experience in at least each of the following areas:

- Agile development practices
- Automated (unit/integration/end-to-end) testing
- Continuous Integration and Continuous Deployment
- Application Protocol Interface (API) development and documentation
- Open-source software development
- Cloud deployment
- Building and testing public facing sites and tools

The references to one or more source code samples must be either links to Git repositories (either credentialed or public) or to equivalent version-controlled repositories that provide CCCM with the full revision history for all files. If an Contractor submits a link to a private Git repository hosted with GitHub, CCCM will provide the Contractor with one or more GitHub user identities by email, and the Contractor will be expected to promptly provide the identified user(s) with access to the private Git repository.

The source code samples should be for projects that are similar in size, scope, and complexity to the project contemplated here. The source code must have been developed by either (i) the Contractor itself, or (ii) an individual that is being proposed as Key Personnel for this project.

6.2.2 Price Submissions

Price submissions must set forth a single dollar amount that represents the Contractor's estimate of the total cost to CCCM for the development services for a base 12 month and 2 option periods. [Instructions on providing price quote, typically an excel workbook, will be included in the final RFQ]. CCCM expects that the labor

categories and staffing levels set forth by the Contractor in the Excel workbook will be consistent with the Contractor's staffing plan.

The Contractor will be compensated at loaded hourly rates. CCCM intends to evaluate quotes and award based on initial quotes, and therefore the Contractor's initial quote should contain the Contractor's best terms.

6.2.3 Interviews

Each interview will be conducted remotely via video connection and/or teleconference. CCCM will communicate with certain Contractors to schedule the dates and times of interviews.

Each interview will include an unstructured question and answer session, during which Contractors will be asked questions about the technical aspects of their quoteand their approach to software development. CCCM expects these interviews will assist CCCM to assess the technical abilities of the proposed development team and to better understand the proposed technical approach described in the Contractor's written submission. Both of the Contractor's proposed Key Personnel must participate in the interview.

The Introductions phase of each interview will last approximately 5 minutes, during which the Contractor and CCCM interview team members will introduce themselves.

The Open Technical Session of each interview will last approximately 45 minutes, during which the Contractor interview team will respond to CCCM’s questions related to the technical aspects of the Contractor's quote. Contractors will NOT be able to use or present any slides, graphs, charts, or other written presentation materials, including handouts. There will be no follow-up session for further questions after this part of the interview.

The Closing Remarks phase of each interview will last approximately 5 minutes, during which the Contractor may make a short presentation summarizing the Contractor's responses to CCCM’s questions.

Interviews will not constitute discussions. Statements made during an interview will not become part of the agreement.

6.2.4 Basis of Award and Evaluation Factors

Each submission received by the Government will be evaluated for technical acceptability. Submissions that are determined to not be technically acceptable after the Contractor has been given the opportunity for a clarification will not be evaluated further.

Quotes must be realistic with respect to technical approach, staffing approach, and total price. Quotes that indicate a lack of understanding of the project requirements may not be considered for award. Quotes may indicate a lack of understanding of the project requirements if the staffing plan does not use a realistic mix of labor categories and hours, or if any proposed hourly labor rates are unrealistically high or low.

The Government will evaluate quotes that are technically acceptable on a competitive best value basis using a trade-off between technical and price factors. Technically acceptable submissions will be evaluated based on four (4) evaluation factors. These factors are:

(1) technical approach,
(2) staffing approach,
(3) similar experience, and
(4) price.

The three (3) technical, non-price evaluation factors, when combined, are significantly more important than price. The Government may make an award to a Contractor that demonstrates an advantage with respect to technical, non-price factors, even if such an award would result in a higher total price to the Government. The importance of price in the evaluation will increase with the degree of equality between Contractors with respect to the non-price factors, or when the Contractor's price is so significantly high as to diminish the value to the Government of the Contractor's advantage in the non-price factors.

6.2.5 Technical Approach

In evaluating a Contractor's technical approach, the Government will consider (a) the quality of the Contractor's plans to provide the open source, agile development services required, (b) the extent of the Contractor's understanding of the details of the project requirements, and (c) the extent to which the Contractor has identified potential

obstacles to efficient development, and has proposed realistic approaches to overcome those potential obstacles.

6.2.6 Staffing Approach

In evaluating a Contractor's staffing approach, the Government will consider (a) the skills and experience of the Key Personnel and other individuals that the Contractor plans to use to provide the required services, (b) the mix of labor categories that will comprise the Contractor's proposed development team, and (c) the Contractor's proposed number of hours of services to be provided by each member of the Contractor's proposed development team.

6.2.7 Similar Experience

In evaluating a Contractor's similar experience, the Government will consider the extent to which the Contractor has recently provided software development services for projects that are similar in size, scope, and complexity to the project described in this RFQ, and the quality of those services. In evaluating the quality of those services, The Government will consider, among other things, the revision history for all files in the source code samples provided. In considering a Contractor's similar experience, the Government may also consider information from any other source, including Contractor's prior customers and public websites.

6.2.8 Price

In evaluating a Contractor's price, the Government will consider the total of the Contractor's estimated costs for the development services for the base and two option periods.

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

IT Security Procedural Guide: Security and Privacy Requirements for IT Acquisition Efforts CIO-IT Security-09-48

Revision 6

April 15, 2021

Office of the Chief Information Security Officer

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

IMPORTANT!

This guide defines security and privacy requirements for GSA IT acquisition contracts involving externally hosted contractor information systems that do not connect to the GSA network; information systems hosted in GSA facilities that directly connect to the GSA network; cloud information systems; or mobile applications. The security and privacy requirements are appropriately formatted to allow the respective security and privacy contract requirements to be placed in-line within a statement of work for each system type. Alternatively, this entire document can be incorporated into the statement of work or contract.

NOTE: Throughout this guide there are highlighted SELECT statements. The requirements office, in coordination with the contracting officer, will complete the selections prior to their incorporation into a contract or statement of work. See example below for the intended use of the SELECT statements.

The guide text states:

1. At the Moderate impact level and higher, the **<SELECT: contractor or Government>** is responsible for providing an independent Security Assessment/Risk Assessment in accordance with GSA IT Security Procedural Guide 06-30, *"Managing Enterprise Cybersecurity Risk."*

The requirements office in coordination with the contracting officer would determine for the specific SOW/contract being prepared whether the contractor or the Government was responsible for the independent assessment and change the statement accordingly. For example, if the contractor is required to provide an independent assessment the statement would state:

1. At the Moderate impact level and higher, the contractor is responsible for providing an independent Security Assessment/Risk Assessment in accordance with GSA IT Security Procedural Guide 06-30, *"Managing Enterprise Cybersecurity Risk."*

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

VERSION HISTORY/CHANGE RECORD

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
		Revision 1 – November 6, 2009		
1	Bo Berlas	Minor Changes to GSA 800-53 R3 Control Tailoring workbook in Appendix A	GSA 800-53 Control Tailoring Workbook Update	17
		Revision 2 – November 7, 2014		
1	John Sitcharing/ Blanche Heard	Minor changes to verbiage regarding Penetration Testing	Update Penetration Testing verbiage	9
2	John Sitcharing/ Blanche Heard	CISO mandated change in Penetration Testing requirement/ naming conventions based on consolidation efforts	CISO Mandate	Entire document
		Revision 3 – February 2, 2017		
1	Bo Berlas	Added Essential Security controls to Section 2	Security Controls Update	9
2	Bo Berlas	Added sections 3-5	Updated to Provide Requirements for Internal Systems, Cloud Systems, and Mobile Applications	22-55
		Revision 4 – January 25, 2018		
1	Bryon Feliksa/ John Klemens	Incorporated security references from MV 16-01 and additional references. Added a section on LiSaaS, Privacy controls, and updated Privacy and other sections to align with GSA policy and procedures.	Incorporate MV 16-01 and consolidate GSA Cybersecurity and Privacy Guidance.	Throughout
		Revision 5 – April 15, 2021		
1	Desai, Klemens, Speidel	Incorporated NDAA/FAR clauses that prohibit the acquisition from covered entities. Added information on coordinating NDAs with OGC and NDA templates. Updated to reflect LiSaaS and External Information System Monitoring guides. Updated guidance regarding a number of controls and deliverables.	Incorporate requirements from the NDAA and FAR, coordination with OGC on NDAs, and updated GSA guidance.	Throughout
2	Berlas, Speidel, Desai, Klemens	Added section on Nonfederal System and Organizations, revised Internal Information Systems definition. Clarified the provision of deliverables.	Incorporate requirements from NIST SP 800-171, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations"	Sections 1 and 7
		Revision 6 – April 15, 2021		
1	Dean	Revisions include: • Updated to NIST SP 800-53, Revision 5 controls		Throughout

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
		Revision 1 – November 6, 2009		
		• Replaced Sensitive But Unclassified with Controlled Unclassified Information • Updated references		

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

APPROVAL

IT Security Procedural Guide 09-48, *"Security and Privacy Requirements for IT Acquisition Efforts,"* Revision 6, is hereby approved for distribution.

X DocuSigned by: Bo Berlas FD717926161544E...

Bo Berlas
GSA Chief Information Security Officer

This guide will be available on the OCISO Webpage and GSA.gov when revised.

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

Table of Contents

1 Introduction....1

1.1 Scope....1
1.2 Purpose....2

2 External Information Systems – IT Security and Privacy Requirements....2

2.1 Required Policies and Regulations for GSA Contracts....2
2.2 GSA Security Compliance Requirements....4
2.3 Essential Security Controls....5
2.4 Assessment and Authorization (A&A) Activities....9
2.5 Reporting and Continuous Monitoring....12
2.6 GSA Privacy Requirements....17
2.7 Additional Stipulations....18

3 Internal Information Systems - IT Security and Privacy Requirements....20

3.1 Required Policies and Regulations for GSA Contracts....20
3.2 GSA Security Compliance Requirements....22
3.3 Essential Security Controls....23
3.4 Assessment and Authorization (A&A) Activities....29
3.5 Reporting and Continuous Monitoring....31
3.6 GSA Privacy Requirements....34
3.7 Additional Stipulations....36

4 Low Impact Software as a Service (LiSaaS) – IT Security and Privacy Requirements....38

4.1 Assessment of the System....38
4.2 Authorization of the System....39
4.3 Maintenance of ATO and Continuous Monitoring....39
4.4 Protection of Information....40
4.5 Data Ownership and Unrestricted Rights to Data....40
4.6 Personally Identifiable Information....41
4.7 Data Availability....41
4.8 Data Release....41
4.9 Confidentiality and Nondisclosure....41
4.10 Section 508 Compliance....42
4.11 Additional Stipulations....42
4.12 Terms of Service....44
4.13 References....44

5 Cloud Information Systems – IT Security and Privacy Requirements....44

5.1 Assessment and Authorization....45
5.2 Assessment of the System....45
5.3 Authorization of the System....47
5.4 Reporting and Continuous Monitoring....49
5.5 Personnel Security Requirements....50
5.6 Sensitive Information Storage....50
5.7 Protection of Information....51
5.7.1 Unrestricted Rights to Data....51

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

5.7.2 Personally Identifiable Information 51
5.7.3 Data Availability 52
5.7.4 Data Release 52
5.8 Data Ownership 52
5.9 Confidentiality and Nondisclosure 52
5.10 GSA Non-Disclosure Agreement 53
5.11 Additional Stipulations 53
5.12 References 55

6 Mobile Application - IT Security and Privacy Requirements 56

6.1 General Mobile Application Guidelines 56
6.2 Mobile Device Security 56
6.3 Application Sources 57
6.4 Terms of Service (ToS) 58
6.5 GSA Privacy Requirements 58
6.6 GSA App Development, Assessment, Authorization and Deployment 59
6.7 Intellectual Property 61
6.8 Confidentiality and Nondisclosure 61
6.9 GSA Non-Disclosure Agreement 62
6.10 Personnel Security Requirements 62
6.11 Additional Stipulations 63

7 Nonfederal Systems and Organizations – IT Security and Privacy Requirements 65

7.1 Required Policies and Regulations for GSA Contracts 65
7.2 GSA Security Compliance Requirements 66
7.3 Security Assessment Activities and Required Documentation 67
7.4 Reporting and Continuous Monitoring 68
7.5 Privacy Assessment Activities and Required Documentation 69
7.6 Additional Stipulations 71

Appendix A: GSA Tailoring of NIST 800-53 Controls 72

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

1 Introduction

The U.S. General Services Administration (GSA) must provide information security for the information systems that support the operations and assets of the agency, including those provided or managed by GSA, another agency, contractor, or other source. The Federal Information Security Modernization Act of 2014 (FISMA of 2014) describes Federal agency security and privacy responsibilities as including "information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency." This includes services which are either fully or partially provided; including other agency hosted, outsourced, and cloud computing solutions. Agency information security programs apply to all organizations (sources) which possess or use Federal information – or which operate, use, or have access to Federal information systems (whether automated or manual) – on behalf of a Federal agency, information systems used or operated by an agency or other organization on behalf of an agency. Not all deliverables contain Controlled Unclassified Information (CUI). The contractor has the responsibility for evaluating, categorizing, and marking CUI. When in question, the contractor should use the National Archives and Records Administration (NARA) CUI Registry to help determine the appropriate category, and designation for marking.

1.1 Scope

This guide provides security and privacy requirements for the GSA information system types outlined below:

- **External Information Systems.** External information systems reside in contractor facilities and typically do not connect to the GSA network. External information systems may be government owned and contractor operated or contractor owned and operated on behalf of GSA or the Federal Government (when GSA is the managing agency).
- **Internal Information Systems.** Internal information systems reside on premise in GSA facilities and may connect to the GSA network. Internal systems are operated on behalf of GSA or the Federal Government (when GSA is the managing agency).
- **Low Impact Software as a Service (LiSaaS) Systems.** LiSaaS systems must adhere to GSA IT Security Procedural Guide 16-75, "*Low Impact Software as a Service (SaaS) Authorization Process*." LiSaaS systems are cloud applications that are implemented for a limited duration, involve low or very low/negligible risk and would cause limited harm to GSA, and cost less than $100,000 annually to deploy.
- **Cloud Information Systems**. Includes Infrastructure as a Service (IaaS), Platform as a Service (PaaS), or SaaS. The service offering must be FedRAMP authorized, in-process, or ready; see Section 5 for additional details.
- **Mobile Application.** A mobile application, most commonly referred to as an app, is a type of application software designed to run on a mobile device, such as a smartphone or tablet computer.
- **Nonfederal Systems and Organizations**. A system or organization: (1) when Controlled Unclassified Information (CUI) is resident in a nonfederal system and organization; (2) not collecting or maintaining information on behalf of a federal agency or using or

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

operating a system on behalf of an agency[1]; and (3) where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or governmentwide policy for the CUI category listed in the CUI Registry.

1.2 Purpose

The purpose of this document is to define and establish consistent security and privacy requirements for GSA IT acquisition contracts involving externally hosted information systems that do not connect to the GSA network; information systems hosted in GSA facilities that may connect to the GSA network; LiSaaS systems, cloud information systems; mobile applications; and nonfederal systems with CUI. The security and privacy requirements are appropriately formatted to allow the respective security and privacy contract language to be placed in-line within a statement of work for each system type. The security and privacy requirements identified in this guide will ensure compliance with the appropriate provisions of FISMA of 2014, OMB Circular A-130, and NIST Special Publication (SP) 800-53, Revision 5.

2 External Information Systems – IT Security and Privacy Requirements

2.1 Required Policies and Regulations for GSA Contracts

Federal Laws, Regulations, and Guidance:

The contractor shall comply with all applicable Federal Laws and Regulations.

- 40 U.S.C. 11331, "*Responsibilities for Federal Information Systems Standards*"
- Executive Order (EO) 13556, "*Controlled Unclassified Information"*
- FISMA of 2014, "*The Federal Information Security Modernization Act of 2014*"
- HSPD 12, "*Homeland Security Presidential Directive 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*"
- OMB Circular A-130, "*Managing Information as a Strategic Resource*"
- OMB M-08-23, "*Securing the Federal Government's Domain Name System Infrastructure (Submission of Draft Agency Plans Due by September 5, 2008)*"
- OMB M 14-03, "*Enhancing the Security of Federal Information and Information Systems*"
- OMB M-10-23, "*Guidance for Agency Use of Third-Party Websites and Applications*"
- OMB M-15-13, "*Policy to Require Secure Connections across Federal Websites and Web Services*"
- OMB M-17-12, "*Preparing for and Responding to a Breach of Personally Identifiable Information*"
- Privacy Act of 1974, "*5 USC, § 552a*"
- National Archives and Records Administration (NARA) Controlled Unclassified Information (CUI) Registry

[1] Nonfederal organizations that collect or maintain information on behalf of a federal agency or that use or operate a system on behalf of an agency, must comply with the requirements in FISMA of 2014, including the requirements in FIPS 200 and the security controls in NIST SP 800-53. (See [44 USC 3554] (a)(1)(A) and Section 2.1 for referenced documents).

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

- OMB Memoranda, location of current fiscal year guidance on Federal Information Security and Privacy Management Requirements, including FISMA reporting

Federal Standards and Guidance:

The contractor shall comply with all applicable Federal Information Processing Standards (FIPS). NIST Special Publications (800 Series) are guidance, unless required by a FIPS publication, in which case usage is mandatory.

- 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*"
- FIPS PUB 140-2[2], "*Security Requirements for Cryptographic Modules*"
- FIPS PUB 140-3, "*Security Requirements for Cryptographic Modules*"
- NIST SP 800-18, Revision 1, "*Guide for Developing Security Plans for Federal Information Systems*"
- NIST SP 800-30, Revision 1, "*Guide for Conducting Risk Assessments*"
- NIST SP 800-34, Revision 1, "*Contingency Planning Guide for Federal Information Systems*"
- NIST SP 800-37, Revision 2, "*Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*"
- NIST SP 800-47, "*Security Guide for Interconnecting Information Technology Systems*"
- NIST SP 800-53, Revision 5, "*Security and Privacy Controls for Information Systems and Organizations*"
- NIST SP 800-53A, Revision 4[3], *"Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*"
- NIST SP 800-63-3, "*Digital Identity Guidelines*"
- NIST SP 800-122, "*Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*"
- NIST SP 800-137, "*Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*"
- NIST SP 800-161, "*Supply Chain Risk Management Practices for Federal Information Systems and Organizations"*

GSA Policies:

The contractor shall comply with the following GSA Directives/Policies.

- GSA Order CIO 1878.3, "*Developing and Maintaining Privacy Threshold Assessments, Privacy Impact Assessments, Privacy Act Notices, and System of Records Notices*"

[2] NIST has issued FIPS 140-3, FIPS 140-2 modules are still being validated and will be accepted through September 22, 2026. For additional information see the NIST cryptographic module validation program webpage.
[3] When NIST SP 800-53A, Revision 5 is final, assessments shall be aligned to it.

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

- GSA Order CIO 2100.1, "*GSA Information Technology (IT) Security Policy*"
- GSA Order CIO 2200.1, "*GSA Privacy Act Program*"
- GSA Order CIO 9297.2, "*GSA Information Breach Notification Policy*"

The GSA policies listed in this paragraph must be followed, if applicable.

- GSA Order CIO 2103.1, "*Controlled Unclassified Information (CUI) Policy*"
- GSA Order CIO 2104.1, "*GSA Information Technology (IT) General Rules of Behavior*"
- GSA Order CIO 2182.2, "*Mandatory Use of Personal Identity Verification (PIV) Credentials*"

GSA Procedural Guides:

GSA IT Procedural Guides are guidance, unless required by a GSA Directive/Policy, in which case usage is mandatory.

Note: GSA's Procedural Guides are updated frequently; to make sure you have the most recent version of publicly available procedural guides, visit GSA.gov. If a non-publicly available guide is needed, contact the contracting officer who will coordinate with the GSA Office of the Chief Information Security Officer to determine if it can be made available.

2.2 GSA Security Compliance Requirements

FIPS PUB 200, *"Minimum Security Requirements for Federal Information and Information Systems*," is a mandatory federal standard that defines the minimum security requirements for federal information and information systems in seventeen security-related areas. Information systems supporting GSA must meet the minimum security and privacy requirements through the use of security controls in accordance with NIST Special Publication 800-53, Revision 5 (hereafter described as NIST 800-53), *"Security and Privacy Controls for Information Systems and Organizations."*

To comply with the Federal standard, GSA must determine the security category of the information and information system in accordance with FIPS PUB 199, *"Standards for Security Categorization of Federal Information and Information Systems,"* and then the contractor shall apply the appropriately tailored set of Low, Moderate, or High impact baseline security controls in NIST 800-53, as determined by GSA. NIST 800-53 controls requiring organization-defined parameters (i.e., password change frequency) shall be consistent with GSA specifications. The GSA-specified control parameters and supplemental guidance defining more specifically the requirements per FIPS PUB 199 impact level are available in the GSA Control Tailoring Workbook referenced in Appendix A of this document.

The Contractor shall use GSA technical guidelines, NIST guidelines, Center for Internet Security (CIS) guidelines (Level 1), or industry best practice guidelines in hardening their systems.

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

2.3 Essential Security Controls

All NIST 800-53 controls must be implemented as per the applicable FIPS PUB 199 Low, Moderate, or High baseline. The following table identifies essential security controls from the respective baselines to highlight their importance and ensure they are implemented. The Contractor shall make the proposed system and security architecture of the information system available to the Security Engineering Division, in the Office of the Chief Information Security Officer for review and approval before commencement of system build (architecture, infrastructure, and code).

Control ID	Control Title	Baseline	GSA Implementation Guidance (if applicable)
AC-2	Account Management	L, M, H	
AC-17 (3)	Remote Access | Managed Access Control Points	M, H	All remote accesses from internal users/systems to the external information system must be routed through GSA's managed network access control points, subjecting them to security monitoring.
AU-2	Event Logging	L, M, H	Information systems shall implement audit configuration requirements as documented in applicable GSA IT Security Technical Hardening Guides (i.e., hardening and technology implementation guides); for web applications see GSA IT Security Procedural Guide 07-35, Section 2.8.10, What to Log. For technologies where a Technical Guide and Standard does not exist, events from an industry source such as vendor guidance or Center for Internet Security benchmark, recommended by the GSA S/SO or Contractor to be approved and accepted by the GSA AO shall be used.
CM-6	Configuration Settings	L, M, H	Information systems, including vendor owned/operated systems on behalf of GSA, shall configure their systems in agreement with GSA technical guidelines, NIST guidelines, Center for Internet Security guidelines (Level 1), or industry best practice guidelines, as reviewed and accepted by the GSA AO.
CP-7	Alternate Processing Site	M, H	FIPS PUB 199 Moderate and High impact systems must implement processing across geographically-disparate locations to ensure fault tolerance. Cloud Infrastructure as a Service (IaaS) architectures shall implement a multi-region strategy (multiple availability zones in a single region are not sufficient).
CP-8	Telecommunications Services	M, H	FIP PUB 199 Moderate and High impact information systems must implement alternate telecom services to support resumption when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

Control ID	Control Title	Baseline	GSA Implementation Guidance (if applicable)
IA-2 (1)	Identification and Authentication (Organizational Users) | Multifactor Authentication to Privileged Accounts	L, M, H	All information systems shall implement multi-factor authentication for privileged accounts.
IA-2 (2)	Identification and Authentication (Organizational Users) | Multifactor Authentication to Non-Privileged Accounts	L, M, H	All information systems must implement multi-factor authentication for non-privileged accounts.
IA-7	Cryptographic Module Authentication	L, M, H	The information system shall implement FIPS PUB 140-2 compliant encryption modules for authentication functions. Reference: Cryptographic Module Validation Program Validated Modules
MP-4	Media Storage	M, H	Digital media including magnetic tapes, external/removable hard drives, flash/thumb drives, diskettes, compact disks and digital video disks shall be encrypted using a FIPS PUB 140-2 certified encryption module.
MP-5	Media Transport	M, H	Digital media including magnetic tapes, external/removable hard drives, flash/thumb drives and digital video disks shall be encrypted using a FIPS PUB 140-2 certified encryption module during transport outside of controlled areas.
PL-8	Security and Privacy Architectures	L, M, H	All information system security architectures must be formally reviewed and approved by the Office of the Chief Information Security Officer, Security Engineering Division during the system develop/design stages of the SDLC and prior to Security Assessment and Authorization.
RA-5	Vulnerability Monitoring and Scanning	L, M, H	All systems must complete the following vulnerability scans: ○ Weekly authenticated scans of operating systems (OS)-including databases ○ Monthly unauthenticated scans of web applications ○ Annual authenticated scans of web applications The most recent vulnerability scanning results shall be provided to GSA together with the quarterly POA&M submission.
SA-22	Unsupported System Components	L, M, H	All systems must be comprised of software and hardware components that are fully supported in terms of security patching for the anticipated life of the system; software must be on GSA's Enterprise Architecture IT Standards List.

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

Control ID	Control Title	Baseline	GSA Implementation Guidance (if applicable)
SC-8 / SC-8(1)	Transmission Confidentiality and Integrity Transmission Confidentiality and Integrity | Cryptographic Protection	M, H	Implemented encryption algorithms and cryptographic modules shall be FIPS-approved and FIPS PUB 140-2 validated, respectively. ○ Digital signature encryption algorithms ○ Block cypher encryption algorithms ○ Secure hashing algorithms For web services connections, implement end to end encryption terminating the connection at the web server; connections terminated at a load balancer shall employ re-encryption techniques to ensure end to end encryption. Internet accessible Websites shall implement HTTPS Only with HTTP Strict Transport Security (HSTS), have no weak ciphers, have no weak protocols, and preload .gov domains. (see Binding Operational Directive (BOD) 18-01, Enhance Email and Web Security). SSL/TLS implementations shall align with GSA IT Security Procedural Guide 14-69, *"SSL/TLS Implementation."*
SC-13	Cryptographic Protection	L, M, H	Implemented encryption algorithms and cryptographic modules shall be FIPS-approved and FIPS PUB 140-2 validated, respectively. ○ Digital signature encryption algorithms ○ Block cypher encryption algorithms ○ Secure hashing algorithms
SC-17	Public Key Infrastructure Certificates	M, H	Implement appropriate creation, use, and signing of crypto certs in agreement with GSA IT Security Procedural Guide 14-69, *"SSL/TLS Implementation,"* and NIST Special Publications 800-52, Revision 2 and 1800-16.
SC-18	Mobile Code	M, H	
SC-22	Architecture and Provisioning for Name / Address Resolution Service	L, M, H	Information systems shall be Domain Name System Security Extensions (DNSSEC) compliant. Reference OMB Memorandum M-08-23, which requires all Federal Government departments and agencies that have registered and are operating second level .gov to be DNSSEC.

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

Control ID	Control Title	Baseline	GSA Implementation Guidance (if applicable)
SC-28 (1)	Protection of Information at Rest | Cryptographic Protection	L, M, H	**Systems that process Personally Identifiable Information (PII), Payment Card Industry (PCI) data, Authenticators (e.g., passwords, tokens, keys, certificates, hashes, etc.), and other sensitive data as determined by the AO, shall encrypt that data everywhere (i.e., at file level, database level, at rest, and in transit (see SC-8(1)). For databases, encryption of the whole database, table, column, or field levels is acceptable, as appropriate. Other methods including, but not limited to, application encryption or tokenization is also acceptable. For web services connections, implement end to end encryption terminating the connection at the web server; connections terminated at a load balancer shall employ re-encryption techniques to ensure end to end encryption.** Encryption algorithms shall be FIPS-approved with FIPS-validated encryption modules.
SI-2	Flaw Remediation	L, M, H	All projects and systems must be adequately tested for flaws; all Critical, High, and Moderate risk findings must be remediated prior to go-live. Post go-live, critical/very high vulnerabilities for Internet-accessible IP addresses must be remediated within 15 days, for all other assets critical/very high vulnerabilities must be remediated within 30 days; High vulnerabilities must be remediated within 30 days; Moderate vulnerabilities must be remediated within 90 days.
SI-3	Malicious Code Protection	L, M, H	
SI-4	System Monitoring	L, M, H	
SI-10	Information Input Validation	M, H	All systems accepting input from end users must validate the input in accordance with industry best practices and published guidelines, including GSA IT Security Procedural Guide 07-35, *"Web Application Security,"* and OWASP Top 10 Web Application Security Vulnerabilities.
SR-2	Supply Chain Risk Management Plan	L, M, H	Tier 3 (Information System) level plans for each system should be developed consistent with the template in Appendix E of NIST SP 800-161
SR-6	Supplier Assessment and Reviews	M, H	
PM-21	Accounting of Disclosures	See note below	Requires accounting of disclosures of PII.

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

Control ID	Control Title	Baseline	GSA Implementation Guidance (if applicable)
PM-25	Minimization of Personally Identifiable Information Used in Testing, Training, and Research	See note below	Requires implementation of policies and procedures to minimize PII used in testing, training, and research.
PT-5	Privacy Notice	See note below	Privacy notices help inform individuals about how their personally identifiable information is being processed by the system or organization
PT-5 (2)	Privacy Notice | Privacy Act Statements	See note below	Include Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.
PT-6	System of Records Notice	See note below	Federal agencies must publish a system of records notice in the Federal Register upon the establishment and/or modification of a Privacy Act system of record
PT-7 (1)	Specific Categories of Personally Identifiable Information | Social Security Numbers	See note below	Federal law and policy establish specific requirements for organizations' processing of Social Security numbers; organizations take steps to eliminate unnecessary uses of Social Security numbers and other sensitive information, and observe any particular requirements that apply.
RA-8	Privacy Impact Assessments	See note below	Conduct privacy impact assessments for systems, programs, or other activities before developing or procuring information technology that will process PII or before initiating a new collection of PII
SI-12 (1)	Information Management and Retention | Limit Personally Identifiable Information Elements	See note below	Limit personally identifiable information being processed in the information life cycle to specified elements.

Note: Privacy controls are not associated with a baseline. Controls are applicable/not applicable based on PII data being collected, stored, or transmitted.

2.4 Assessment and Authorization (A&A) Activities

The implementation of a new Federal Government IT system requires a formal approval process known as Assessment and Authorization (A&A). NIST Special Publication 800-37, Revision 2 (hereafter described as NIST 800-37) and GSA IT Security Procedural Guide 06-30, "*Managing Enterprise Cybersecurity Risk,*" provide guidelines for performing the A&A process. The Contractor system/application must have a valid assessment and authorization, known as

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

an Authorization to Operate (ATO) (signed by the Federal government) before going into operation and processing GSA information. The failure to obtain and maintain a valid ATO will result in the termination of the contract. The system must have a new A&A conducted (signed by the Federal government) when significant changes are made to the system, and as specified in GSA IT Security Procedural Guide 06-30, "*Managing Enterprise Cybersecurity Risk,*" and the guides for GSA's other A&A processes referenced therein.

Assessing the System

1. The Contractor shall comply with Assessment and Authorization (A&A) requirements as mandated by Federal laws and policies, including making available any documentation, physical access, and logical access needed to support this requirement. The Level of Effort for the A&A is based on the System's NIST Federal Information Processing Standard (FIPS) Publication 199 categorization. Documents that contain CUI must be marked as such. Not all deliverables contain CUI. When in question, the contractor should use the NARA CUI Registry to help determine the appropriate designation for marking, handling or transmitting. The contractor shall create, maintain and update the following A&A documentation:

    - System Security and Privacy Plan (SSPP) completed in agreement with NIST Special Publication 800-18, Revision 1, *"Guide for Developing Security Plans for Federal Information Systems*" and completed in accordance with GSA SSPP requirements and templates. The SSPP shall include as appendices required policies and procedures across 19 control families mandated per FIPS PUB 200, Rules of Behavior, and Interconnection Security Agreements (in agreement with NIST Special Publication 800-47, *"Security Guide for Interconnecting Information Technology Systems"*). The SSPP shall include; as an appendix, a completed GSA Control Tailoring Workbook (CTW) identified in Appendix A of this guide. The column in the CTW titled "*Vendor/Contractor Defined Values*" shall be used to document all contractor implemented parameter settings that differ from the GSA Defined Value and the Vendor/Contractor defined value when the value is deferred to the Vendor/Contractor. GSA's approval will be documented in the CTW column titled "*GSA Approval of Vendor/Contractor Defined Values*."
    - Contingency Plan completed in agreement with NIST Special Publication 800-34 and GSA IT Security Procedural Guide 06-29, "*Contingency Planning."*
    - Business Impact Assessment completed in agreement with NIST Special Publication 800-34 and GSA IT Security Procedural Guide 06-29, "*Contingency Planning."*
    - Contingency Plan Test Report completed in agreement with GSA IT Security Procedural Guide 06-29, *"Contingency Planning."*
    - Incident Response Plan completed in agreement with NIST Special Publication 800-61, "*Computer Security Incident Handling Guide*" and GSA IT Security Procedural Guide 01-02, "*Incident Response*."

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

- Incident Response Test Report completed in agreement NIST Special Publication 800-61, "Computer Security Incident Handling Guide" and GSA IT Security Procedural Guide 01-02, "*Incident Response*."
- Configuration Management Plan completed in agreement with GSA IT Security Procedural Guide 01-05, "*Configuration Management*."
- Plan of Action & Milestones completed in agreement with GSA IT Security Procedural Guide 09-44, *"Plan of Action and Milestones (POA&M)."*
- Penetration Test Reports documenting the results of vulnerability analysis and exploitability of identified vulnerabilities. Note: Penetration testing is required for all Internet accessible, all FIPS 199 High, and all High Value Asset (HVA) information systems. These systems are required to complete an independent penetration test and provide an Independent Penetration Test Report documenting the results of the exercise as part of the A&A package. Reference GSA IT Security Procedural Guide 06-30, *"Managing Enterprise Cybersecurity Risk"* and GSA IT Security Procedural Guide 11-51, *"Conducting Penetration Test Exercises"* for penetration testing guidance.

2. Information systems must be assessed and authorized every three (3) years or whenever there is a significant change to the system's security posture in accordance with NIST Special Publication 800-37, Revision 2, " *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy,"* and CIO IT Security 06-30, "*Managing Enterprise Cybersecurity Risk*" or via continuous monitoring based on GSA CIO IT Security 12-66, "*Information Security Continuous Monitoring (ISCM) Strategy & Ongoing Authorization (OA) Program*" that is reviewed and accepted by the GSA CISO.
3. At the Moderate impact level and higher, the **<SELECT: contractor or Government>** is responsible for providing an independent Security Assessment/Risk Assessment in accordance with GSA IT Security Procedural Guide 06-30, *"Managing Enterprise Cybersecurity Risk."*
4. If the Government is responsible for providing a Security Assessment/Risk Assessment and Penetration Test, the Contractor shall allow GSA employees (or GSA designated third party contractors) to conduct A&A activities to include control reviews in accordance with NIST 800-53/NIST 800-53A and GSA IT Security Procedural Guide 06-30, *"Managing Enterprise Cybersecurity Risk."* Review activities include but are not limited to operating system vulnerability scanning, web application scanning, and database scanning of applicable systems that support the processing, transportation, storage, or security of GSA information. This includes the general support system infrastructure.
5. Identified gaps between required NIST 800-53 controls and the contractor's implementation as documented in the Security Assessment/Risk Assessment report shall be tracked for mitigation in a Plan of Action and Milestones (POA&M) document completed in accordance with GSA IT Security Procedural Guide 09-44, *"Plan of Action and Milestones (POA&M)."* Depending on the severity of the gaps, the Government may require them to be remediated before an Authorization to Operate is issued.

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

6. The Contractor is responsible for mitigating all security risks found during the A&A and continuous monitoring activities. Vulnerabilities must be mitigated as follows:

    (1) For Internet-accessible IP addresses
        (a) Any Critical (Very High) scan vulnerabilities must be remediated within 15 days.
        (b) Any High scan vulnerabilities must be remediated within 30 days.
        (c) Any Moderate scan vulnerabilities must be remediated within 90 days.
    (2) For all other assets
        (a) Any Critical (Very High) and High scan vulnerabilities must be remediated within 30 days.
        (b) Any Moderate scan vulnerabilities must be remediated within 90 days.

7. The Government will determine the risk rating of vulnerabilities.

Authorization of the System

1. Upon receipt of the documentation (A&A Package) described in GSA IT Security Procedural Guide 06-30, *"Managing Enterprise Cybersecurity Risk"* and NIST Special Publication 800-37 as documented above, the GSA Authorizing Official (AO) for the system (in coordination with the GSA Chief Information Security Officer (CISO), System Owner, Information System Security Manager (ISSM), and Information System Security Officer (ISSO) will render an authorization decision to:
    - Authorize system operation w/out any restrictions or limitations on its operation;
    - Authorize system operation w/restriction or limitation on its operation, or;
    - Not authorize for operation.
2. The Contractor shall provide access to the Federal Government, or their designee acting as their agent, when requested, in order to verify compliance with the requirements for an Information Technology security program. At its option, the Government may choose to conduct on site surveys. The Contractor shall make appropriate personnel available for interviews and documentation during this review.

2.5 Reporting and Continuous Monitoring

Maintenance of the security authorization to operate will be through continuous monitoring of security controls of the external system and its environment of operation to determine if the security controls in the information system continue to be effective over time in light of changes that occur in the system and environment. Through continuous monitoring, security controls and supporting deliverables are updated and submitted to GSA per the schedules below. The submitted deliverables (or lack thereof) provide a current understanding of the security state and risk posture of the information systems. They allow GSA AOs to make credible risk-based decisions regarding the continued operations of the information systems and initiate appropriate responses as needed when changes occur.

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

Vendor deliverables as identified below will be reviewed and accepted or rejected by the process described in GSA CIO IT Security Procedural Guide 19-101, "*External Information System Monitoring*."

Deliverables to be provided Quarterly to the GSA ISSO, ISSM, and/or COR

1. Vulnerability Monitoring and Scanning
   Reference: NIST 800-53 control RA-5
   Provide the most recent Web Application and Operating System vulnerability scan reports. GSA's control parameter for RA-5, Vulnerability Monitoring and Scanning, specifies the following type and frequency of scans; weekly authenticated scans of operating systems (OS)-including databases, monthly unauthenticated scans of web applications, annual authenticated scans of web applications

2. Plan of Action & Milestones (POA&M) Update
   Reference: NIST 800-53 control CA-5
   Provide POA&M updates in accordance with requirements and the schedule set forth in GSA CIO IT Security Procedural Guide 09-44, "*Plan of Action and Milestones (POA&M).*"

Deliverables to be provided Annually or when there is a major change to the GSA ISSO, ISSM, and/or COR

Note: Deliverables annotated with a "*" below may be attested to via an attestation letter as described in GSA CIO-IT Security-19-101, "*External Information System Monitoring.*"

1. Updated A&A documentation including the System Security and Privacy Plan, Contingency Plan, and Business Impact Analysis
   a. System Security and Privacy Plan
      Reference: NIST 800-53 control PL-2
      Review and update the System Security and Privacy Plan annually to ensure the plan is current and accurately describes implemented system controls and reflects changes to the contractor system and its environment of operation. The System Security and Privacy Plan must be in accordance with NIST 800-18, Revision 1, *"Guide for Developing Security Plans for Federal Information Systems."*
   b. Contingency Plan
      Reference: NIST 800-53 control CP-2
      Provide an annual update to the contingency plan completed in accordance with NIST 800-34, *"Contingency Planning Guide for Federal Information Systems"*, and GSA IT Security Procedural Guide 06-29, *"Contingency Planning."*
   c. Business Impact Analysis
      Reference: NIST 800-53 control CP-2
      Provide an annual update to the business impact analysis completed in accordance with NIST 800-34, *"Contingency Planning Guide for Federal*

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

Information Systems", and GSA IT Security Procedural Guide 06-29, *"Contingency Planning."*

2. User Certification/Authorization Review Documents
   Reference: NIST 800-53 control AC-2
   Provide the results of the annual review and validation of system users' accounts to ensure the continued need for system access. The user certification and authorization documents will illustrate the organization establishes, activates, modifies, reviews, disables, and removes information system accounts in accordance with documented account management procedures.

3. *Separation of Duties Document/Matrix
   Reference: NIST 800-53 control AC-5
   Develop and furnish a separation of duties matrix reflecting proper segregation of duties for IT system maintenance, management, and development processes. The separation of duties matrix will be updated or reviewed on an annual basis.

4. *Information Security Awareness and Training Records
   Reference: NIST 800-53 control AT-4
   Provide the results of the literacy training and awareness (AT-2) and role-based information security technical training (AT-3). AT-2 requires basic security awareness training for employees and contractors that support the operation of the contractor system. AT-3 requires information security technical training to information system security roles. Training shall be consistent with the requirements contained in C.F.R. Part 5 Subpart C (5 C.F.R 930.301) and conducted at least annually.

5. Annual FISMA Self-Assessment
   Reference: NIST 800-53 control CA-2
   Deliver the results of the annual FISMA self-assessment conducted per GSA IT Security Procedural Guide 04-26, "*Federal Information Security Modernization Act (FISMA) Implementation."* Based on the controls selected for self-assessment, the GSA OCISO will provide the appropriate test cases for completion.

6. *System(s) Baseline Configuration Standard Document
   Reference: NIST 800-53 control CM-2
   Provide a well-defined, documented, and up-to-date specification to which the information system is built.

7. System Configuration Settings
   Reference: NIST 800-53 control CM-6/CM-6(1)
   Establish and document mandatory configuration settings for information technology products employed within the information system that reflect the most restrictive mode consistent with operational requirements. Configuration settings are the configurable security-related parameters of information technology products that compose the information system. Systems should be configured in agreement with GSA technical guidelines, NIST guidelines, Center for Internet Security guidelines (Level 1), or industry best practice guidelines in hardening systems, as reviewed and accepted by the GSA AO.

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

Provide the most recent operating system Configuration Settings Compliance scan report.

8. Configuration Management Plan
   Reference: NIST 800-53 control CM-9
   Provide an annual update to the Configuration Management Plan for the information system.

9. Contingency Plan Test Report
   Reference: NIST 800-53 control CP-4
   Provide a contingency plan test report completed in accordance with GSA IT Security Procedural Guide 06-29, *"Contingency Planning."* A continuity test shall be conducted annually prior to mid-July of each year. The continuity test can be a tabletop test while the system is at the FIPS PUB 199 Low Impact level. The tabletop test must include Federal and hosting Contractor representatives. Functional exercises must be completed once every three years for FIPS PUB 199 Moderate impact systems and annually for FIPS PUB 199 High impact systems.

10. Incident Response Test Report
    Reference: NIST 800-53 control IR-3
    Provide an incident response plan test report documenting results of incident reporting process per GSA IT Security Procedural Guide 01-02, *"Incident Response."*

11. Information Exchanges (if applicable)
    Reference: NIST 800-53 control CA-3
    Provide Interconnection Security Agreements (ISA) and supporting Memoranda of Agreement/Understanding (MOA/U), completed in accordance with NIST 800-47, *"Security Guide for Connecting Information Technology Systems,"* if there are existing or new interconnections. Per NIST 800-47, an interconnection is the direct connection of two or more IT systems for the purpose of sharing data and other information resources through a pipe, such as ISDN, T1, T3, DS3, VPN, etc. ISAs shall be submitted as appendices as part of the annual System Security and Privacy Plan submission. ISAs shall include, if applicable, any changes since the last submission; updated ISAs are required at least every three years.

12. *Rules of Behavior
    Reference: NIST 800-53 control PL-4
    Define and establish Rules of Behavior for information system users. Rules of Behavior shall be submitted as an appendix to the System Security and Privacy Plan.

13. Penetration Testing Report
    Reference: NIST 800-53 control CA-8
    All Internet accessible systems, and all FIPS PUB 199 High impact systems are required to complete an independent penetration test and provide a Penetration Test Report documenting the results of the exercise as part of their A&A package. Annual penetration tests are required for these same systems in accordance with GSA Order CIO 2100.1 and CIO-IT Security-11-51, "*Conducting Penetration Test Exercises.*"

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

14. *Personnel Screening and Security
    Reference: NIST 800-53 control PS-3, NIST 800-53 control PS-7
    Furnish documentation reflecting favorable adjudication of background investigations for all personnel (including subcontractors) supporting the system. Contractors shall comply with GSA Order CIO 2100.1, *"GSA Information Technology (IT) Security Policy"* and GSA Order ADM 2181.1, "*Homeland Security Presidential Directive-12, Personal Identity Verification and Credentialing, and Background Investigations for Contractors."* GSA separates the risk levels for personnel working on Federal computer systems as follows:

    - A favorable initial fitness/suitability determination must be granted and a Tier 1 or higher background investigation initiated before access to the GSA network or any GSA IT system. There shall be no waivers to this requirement for GSA network and IT system access for GSA employees or contractors.
    - A favorable initial fitness/suitability determination must be granted and a Tier 2 or higher background investigation initiated before access to PII/CUI is granted. The authority and access shall be determined by the appropriate GSA Supervisor (for GSA employees) or CO (for contract personnel), Data Owner, and the System's AO. Each System's AO, with the request of the GSA Supervisor, Data Owner or CO, shall evaluate the risks associated with each such request.
    - A favorable suitability determination must be completed at a Tier 2 or higher background investigation before privileged access to the GSA network or IT systems is granted. A waiver may be requested in order to maintain GSA business operations; however such requests should be used judiciously and not incur unnecessary risks to GSA.

    If final adjudication of a background investigation is unfavorable, GSA network and IT system access must be revoked, and any GFE, including the GSA PIV card, must be retrieved and returned to OMA.

Deliverables to be provided Biennially to the GSA ISSO, ISSM, and/or COR

Note: Deliverables annotated with a "*" below may be attested to via an attestation letter as described in GSA CIO IT Security Procedural Guide 19-101, "*External Information System Monitoring.*"

1. Policies and Procedures
   Develop and maintain policies and procedures for the following control families:
   a. *Access Control (NIST 800-53 AC-1 Policy and Procedures)
   b. *Awareness and Training (NIST 800-53 AT-1 Policy and Procedures)
   c. *Audit and Accountability (NIST 800-53 AU-1 Policy and Procedures)
   d. *Identification and Authentication (NIST 800-53 IA-1 Policy and Procedures)
   e. *Incident Response (NIST 800-53 IR-1 Policy and Procedures) - reporting timeframes are documented in GSA IT Security Procedural Guide 01-02, "*Incident Response*"
   f. *System Maintenance (NIST 800-53 MA-1 Policy and Procedures)

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

g. *Media Protection (NIST 800-53 MP-1 Policy and Procedures)
h. *Physical and Environmental Protection (NIST 800-53 PE-1 Policy and Procedures)
i. *Personnel Security (NIST 800-53 PS-1 Policy and Procedures)
j. *PII Processing and Transparency (NIST 800-53 PT-1 Policy and Procedures) (if applicable)
k. *System and Information Integrity (NIST 800-53 SI-1 Policy and Procedures)
l. *System and Communication Protection (NIST 800-53 SC-1 Policy and Procedures)
m. *Key Management Policy (NIST 800-53 SC-12 Cryptographic Key Establishment and Management)
n. *Supply Chain Risk Management (NIST 800-53 SR-1 Policy and Procedures)

2.6 GSA Privacy Requirements

Personally identifiable information (PII) **<SELECT: is or is not>** in the scope of the acquisition and PII **<SELECT: is or is not>** expected to be stored, processed, or transmitted in the vendor's information system. The collection, maintenance or dissemination of any PII that is subject to the Privacy Act and/or the E-Government Act will be handled in full accordance with all GSA rules of conduct and in accordance with GSA Privacy Program requirements.

The contractor shall work with GSA to prepare a Privacy Threshold Assessment (PTA) to confirm and document PII is not in scope, or to determine which categories of information will be stored, processed, or transmitted by the system. The PTA must be completed before development begins and whenever a change with a privacy impact (e.g., a new category of information is collected) is made to an existing system. PTAs are required as part of GSA's process to determine whether a Privacy Impact Assessment (PIA) and/or a System of Records Notice (SORN) is required, and if any other privacy requirements apply to the information system. Information regarding PIAs can be found in this GSA Policy.

PII (should it come into scope) will require the following guidelines be adhered to.

- The vendor's information system must be authorized at least at the FIPS PUB 199 Moderate level.
- For any system that collects, maintains or disseminates PII, a PIA must be completed by the contractor and provided to the GSA Privacy Office for review along with the other authorization to operate (ATO) documents.
- If the system retrieves information using PII, the Privacy Act applies and it must have a system of records notice (SORN) published in the Federal Register.
- If PII is collected from individuals by the system, a Privacy Act Statement (i.e., Privacy Notice) must be provided to users prior to their use of the application on what data is being collected and why, as well as the authority for the collection and the impact of not providing some or all of it. The Privacy Act Statement must be available to the individual directly on the form used to collect the information. Providing a link back to the Statement from the form is acceptable.

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

Per OMB A-130 Privacy Act Statements must include:

(1) the authority (whether granted by statute or executive order) that authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary;
(2) the principal purpose(s) for which the information is intended to be used;
(3) the published routine uses to which the information is subject;
(4) the effects on the individual, if any, of not providing all or any part of the requested information; and
(5) an appropriate citation (and, if practicable, a link) to the relevant SORN(s).

An example Privacy Act Statement is available at GSA's Privacy Act Statement for Design Research webpage.

Note: Systems that access data a user creates must assume a user may include privacy data/PII in the system unless the data creation is restricted to data controlled by the system.

All contractor staff who have significant privacy information responsibilities must complete GSA's mandatory privacy awareness and role-based training courses. This includes contractors who work with PII as part of their work duties (e.g., Human Resource staff, Finance staff, and managers/supervisors).

2.7 Additional Stipulations

1. When containing sensitive information, deliverables shall be labeled Controlled Unclassified Information (CUI) or contractor selected designation per document sensitivity. Not all deliverables contain CUI. When in question, the contractor should use the National Archives and Records Administration (NARA) CUI Registry to help determine the appropriate designation for marking. External transmission/dissemination of CUI to or from a Government computer must be encrypted. Certified encryption modules must be used in accordance with FIPS PUB 140-2, *"Security Requirements for Cryptographic Modules."*
2. The Contractor shall certify applications are fully functional and operate correctly as intended on systems using benchmarks from GSA technical guidelines, NIST guidelines, Center for Internet Security guidelines, or industry best practice guidelines, as reviewed and accepted by the GSA AO. The standard installation, operation, maintenance, update, and/or patching of software shall not alter the configuration settings from the approved benchmark configuration. Information technology for Windows systems should use the Windows Installer Service for installation to the default "program files" directory and should be able to silently install and uninstall. Applications designed for normal end users shall run in the standard user context without elevated system administration privileges. The contractor shall use tools to verify their products operate correctly with the approved benchmark configurations and do not alter the benchmark settings.

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

3. The Contractor shall cooperate in good faith in defining non-disclosure agreements (NDAs) that other third parties must sign when acting as the Federal government's agent.

Note: GSA's Office of the General Counsel (OGC) is available to coordinate on defining NDA requirements. Upon request, GSA OGC can advise on NDA development.

4. The Government has the right to perform manual or automated audits, scans, reviews, or other inspections of the vendor's IT environment being used to provide or facilitate services for the Government. The Contractor shall be responsible for the following privacy and security safeguards:

    a. The Contractor shall not publish or disclose in any manner, without the Contracting Officer's written consent, the details of any safeguards either designed or developed by the Contractor under this contract or otherwise provided by the Government. Exception - Disclosure to a Consumer Agency for purposes of A&A verification or to the MAX.Gov portal. To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data, the Contractor shall afford the Government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases within 72 hours of the request. Access to support incident investigations, shall be provided as soon as possible but not longer than 72 hours after request.

    The program of inspection shall include, but is not limited to:

    - Authenticated and unauthenticated operating system/network vulnerability scans
    - Authenticated and unauthenticated web application vulnerability scans
    - Automated scans can be performed by Government personnel, or agents acting on behalf of the Government, using Government operated equipment, and Government specified tools. If the vendor chooses to run its own automated scans or audits, results from these scans may at the Government's discretion, be accepted in lieu of Government performed vulnerability scans. In these cases, scanning tools and their configuration shall be approved by the Government. In addition, the results of vendor-conducted scans shall be provided in full to the Government.

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

5. The Contractor shall comply with Section 1634 of Public Law 115-91 that prohibits use of any hardware, software, or services developed or provided, in whole or in part, by— (1) Kaspersky Lab (or any successor entity); (2) any entity that controls, is controlled by, or

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

is under common control with Kaspersky Lab; or (3) any entity of which Kaspersky Lab has majority ownership.

6. The Contractor shall comply with 52.204-25 of the Federal Acquisition Regulation (FAR). It prohibits, under Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232), contractors from providing to the Government any equipment, system, or service that uses telecommunications equipment or video surveillance services from certain named companies as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception or waiver is granted per the FAR. It also prohibits, under Section 889(a)(1)(B), contractors from using any equipment, system, or service that uses telecommunications or video surveillance equipment or services from certain named companies as a substantial or essential component of any system or as critical technology as part of any system, unless an exception or waiver is granted per the FAR. The proscribed companies are Huawei Technologies Company, ZTE Corporation, Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, and Dahua Technology Company and their subsidiaries and affiliates.

3 Internal Information Systems - IT Security and Privacy Requirements

3.1 Required Policies and Regulations for GSA Contracts

Federal Laws, Regulations, and Guidance:

The contractor shall comply with all applicable Federal Laws and Regulations.

- 40 U.S.C. 11331, "*Responsibilities for Federal Information Systems Standards*"
- FISMA of 2014, "*The Federal Information Security Modernization Act of 2014*"
- HSPD 12, "*Homeland Security Presidential Directive 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*"
- OMB Circular A-130, "*Managing Information as a Strategic Resource*"
- OMB M-08-23, "*Securing the Federal Government's Domain Name System Infrastructure (Submission of Draft Agency Plans Due by September 5, 2008)*"
- OMB M 14-03, "*Enhancing the Security of Federal Information and Information Systems*"
- OMB M-10-23, "*Guidance for Agency Use of Third-Party Websites and Applications*"
- OMB M-15-13, "*Policy to Require Secure Connections across Federal Websites and Web Services*"
- OMB M-17-12, "*Preparing for and Responding to a Breach of Personally Identifiable Information*"
- Privacy Act of 1974, "*5 USC, § 552a*"
- National Archives and Records Administration (NARA) Controlled Unclassified Information (CUI) Registry
- OMB Memoranda, location of current fiscal year guidance on Federal Information Security and Privacy Management Requirements, including FISMA reporting

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

Federal Standards and Guidance:

The contractor shall comply with all applicable Federal Information Processing Standards (FIPS). NIST Special Publications (800 Series) are guidance, unless required by a FIPS publication, in which case usage is mandatory.

- 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*"
- FIPS PUB 140-2[4], "*Security Requirements for Cryptographic Modules*"
- FIPS PUB 140-3, "*Security Requirements for Cryptographic Modules*"
- NIST SP 800-18, Revision 1, "*Guide for Developing Security Plans for Federal Information Systems*"
- NIST SP 800-30, Revision 1, "*Guide for Conducting Risk Assessments*"
- NIST SP 800-34, Revision 1, "*Contingency Planning Guide for Federal Information Systems*"
- NIST SP 800-37, Revision 2, "*Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*"
- NIST SP 800-47, "*Security Guide for Interconnecting Information Technology Systems*"
- NIST SP 800-53, Revision 5, "*Security and Privacy Controls for Information Systems and Organizations*"
- NIST SP 800-53A, Revision 4[5], *"Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*"
- NIST SP 800-63-3, "*Digital Identity Guidelines*"
- NIST SP 800-122, "*Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*"
- NIST SP 800-137, "*Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*"
- NIST SP 800-161, "*Supply Chain Risk Management Practices for Federal Information Systems and Organizations"*

GSA Policies:

The contractor shall comply with the following GSA Directives/Policies.

- GSA Order CIO 1878.3, "*Developing and Maintaining Privacy Threshold Assessments, Privacy Impact Assessments, Privacy Act Notices, and System of Records Notices*"
- GSA Order CIO 2100.1, "*GSA Information Technology (IT) Security Policy*"
- GSA Order CIO 2200.1, "*GSA Privacy Act Program*"
- GSA Order CIO 9297.2, "*GSA Information Breach Notification Policy*"

[4] NIST has issued FIPS 140-3, FIPS 140-2 modules are still being validated and will be accepted through September 22, 2026. For additional information see the NIST cryptographic module validation program webpage.
[5] When NIST SP 800-53A, Revision 5 is final, assessments shall be aligned with it.

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

The contractor shall comply with the following GSA policies listed below when inside a GSA building or inside a GSA firewall.

- GSA Order CIO 2100.3, "*Mandatory Information Technology (IT) Security Training Requirement for Agency and Contractor Employees with Significant Security Responsibilities*"
- GSA Order ADM 9732.1, "*Personnel Security and Suitability Program Handbook*"

The GSA policies listed in this paragraph must be followed, if applicable.

- GSA Order CIO 2103.1, "*Controlled Unclassified Information (CUI) Policy*"
- GSA Order CIO 2104.1, "*GSA Information Technology (IT) General Rules of Behavior*"
- GSA Order CIO 2182.2, "*Mandatory Use of Personal Identity Verification (PIV) Credentials*"

GSA Procedural Guides:

GSA IT Procedural Guides are guidance, unless required by a GSA Directive/Policy, in which case usage is mandatory.

Note: GSA's Procedural Guides are updated frequently; to make sure you have the most recent version of publicly available procedural guides, visit GSA.gov. If a non-publicly available guide is needed, contact the contracting officer who will coordinate with the GSA Office of the Chief Information Security Officer to determine if it can be made available.

3.2 GSA Security Compliance Requirements

FIPS PUB 200, *"Minimum Security Requirements for Federal Information and Information Systems,"* is a mandatory federal standard that defines the minimum security requirements for federal information and information systems in seventeen security-related areas. Information systems supporting GSA must meet the minimum security and privacy requirements through the use of the security controls in accordance with NIST Special Publication 800-53, Revision 5 (hereafter described as NIST 800-53), *"Security and Privacy Controls for Information Systems and Organizations."*

To comply with the federal standard, GSA must determine the security category of the information and information system in accordance with FIPS PUB 199, *"Standards for Security Categorization of Federal Information and Information Systems,"* and then the contractor shall apply the appropriately tailored set of Low, Moderate, or High impact baseline security controls in NIST 800-53, as determined by GSA. NIST 800-53 controls requiring organization-defined parameters (i.e., password change frequency) shall be consistent with GSA specifications. The GSA-specified control parameters and supplemental guidance defining more specifically the requirements per FIPS PUB 199 impact level are available in the GSA Control Tailoring Workbook referenced in Appendix A of this document.

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

The Contractor shall use GSA technical guidelines, NIST guidelines, Center for Internet Security (CIS) guidelines (Level 1), or industry best practice guidelines in hardening their systems. Where a GSA security hardening benchmark exists, it must be used. GSA security hardening benchmarks may be exceeded but not lowered. GSA benchmarks are available on the GSA Intranet and will be provided by GSA upon request.

3.3 Essential Security Controls

All NIST 800-53 controls must be implemented as per the applicable FIPS PUB 199 Low, Moderate, or High baseline. The following table identifies essential security controls from the respective baselines to highlight their importance; ensure they are implemented; and identify integration requirements with GSA's IT and IT Security environment. Systems shall have these essential security controls implemented. Further, the proposed system and security architecture of the information system shall be reviewed and approved by the Security Engineering Division, in the Office of the Chief Information Security Officer before commencement of system build (architecture, infrastructure, and code).

Control ID	Control Title	Baseline	GSA Implementation Guidance
AC-2	Account Management	L, M, H	Account management systems must leverage or integrate with existing GSA account management solutions or processes, as applicable and defined in the GSA IT ICAM Roadmap (see CIO IL-20-01, "*Enterprise Identity, Credential, and Access Management [ICAM] Policy*").
AC-17 (3)	Remote Access | Managed Access Control Points	M, H	All remote accesses to the internal information system must be routed through GSA's managed network access control points, subjecting them to security monitoring.
AU-2	Event Logging	L, M, H	Information systems shall implement audit configuration requirements as documented in applicable GSA IT Security Technical Hardening Guides (i.e., hardening and technology implementation guides); for web applications see GSA IT Security Procedural Guide 07-35, Section 2.8.10, What to Log. For technologies where a Technical Guide and Standard does not exist, events from an industry source such as vendor guidance or Center for Internet Security (CIS) benchmark, recommended by the GSA S/SO or Contractor to be approved by the GSA AO shall be used. Internal Information systems shall transmit OS audit log events to GSA's Enterprise Logging Platform (ELP) when possible. OS audit logs not able to be transmitted to the ELP, web application, database, and other logs will be retained by the system owner.

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

Control ID	Control Title	Baseline	GSA Implementation Guidance
AU-6 (1)	Audit Record Review, Analysis, and Reporting | Automated Process Integration	M, H	Internal systems must integrate with GSA's Security Stack as specified in GSA IT Security Procedural Guide 06-30, *"Managing Enterprise Cybersecurity Risk,"* which supports review of OS audit log events via GSA's Enterprise Logging Platform (ELP). OS audit logs not able to be transmitted to the ELP, web application, database, and other logs will be reviewed by the system owner.
CM-6	Configuration Settings	L, M, H	Information systems shall implement GSA benchmarks for system hardening. GSA benchmarks may be exceeded but not lowered. Where a GSA benchmark does NOT exist, GSA technical guidelines, NIST guidelines, Center for Internet Security guidelines (Level 1), or industry best practice guidelines, as reviewed and accepted by the GSA AO. Further, all workstations and servers connected to the GSA network shall have BigFix and have agents installed.
CM-7	Least Functionality	L, M, H	Internal systems must integrate with GSA's Security Stack as specified in GSA IT Security Procedural Guide 06-30, "*Managing Enterprise Cybersecurity Risk*," which supports least functionality via GSA's implementation of Bit9.
CP-7	Alternative Processing Site	M, H	FIPS PUB 199 Moderate and High impact systems must implement processing across geographically disparate locations to ensure fault tolerance. Cloud Infrastructure as a Service (IaaS) architectures shall implement a multi-region strategy (multiple availability zones in a single region are not sufficient).
CP-8	Telecommunications Services	M, H	FIP PUB 199 Moderate and High impact information systems must implement alternate telecom services to support resumption when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.
IA-2 (1)	Identification and Authentication (Organizational Users) | Multifactor Authentication to Privileged Accounts	L, M, H	All information systems shall implement multi-factor authentication for privileged accounts. Information systems shall technically integrate with a GSA privileged access and authentication solution, as applicable and defined in the GSA IT ICAM Roadmap (see CIO IL-20-01, *"Enterprise Identity, Credential, and Access Management [ICAM] Policy*").

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

Control ID	Control Title	Baseline	GSA Implementation Guidance
IA-2 (2)	Identification and Authentication (Organizational Users) | Multifactor Authentication to Non-Privileged Accounts	L, M, H	All information systems must implement multi-factor authentication for non-privileged accounts. Information systems shall technically integrate with a GSA supported enterprise authentication solution (e.g., support SAML 2.0 or OIDC with an GSA enterprise SSO solution), , as applicable and defined in the GSA IT ICAM Roadmap (see CIO IL-20-01, "*Enterprise Identity, Credential, and Access Management [ICAM] Policy*").
IA-7	Cryptographic Module Authentication	L, M, H	The information system shall implement FIPS PUB 140-2 compliant encryption modules for authentication functions. Reference: Cryptographic Module Validation Program Validated Modules
MP-4	Media Storage	M, H	Digital media including magnetic tapes, external/removable hard drives, flash/thumb drives, diskettes, compact disks and digital video disks shall be encrypted using a FIPS PUB 140-2 certified encryption module.
MP-5	Media Transport	M, H	Digital media including magnetic tapes, external/removable hard drives, flash/thumb drives and digital video disks shall be encrypted using a FIPS PUB 140-2 certified encryption module during transport outside of controlled areas.
PL-8	Security and Privacy Architectures	L, M, H	All information system security architectures must be formally reviewed and approved by the Office of the Chief Information Security Officer, Security Engineering Division during the system develop/design stages of the SDLC and prior to Security Assessment and Authorization.
RA-5	Vulnerability Monitoring and Scanning	L, M, H	All systems must integrate with the GSA vulnerability scanning tool set managed by the Security Operations Division in the Office of the Chief Information Security Officer. Information systems shall coordinate integration with the scanning program by contacting SecOps@gsa.gov.
SA-22	Unsupported System Components	L, M, H	All systems must be comprised of software and hardware components that are fully supported in terms of security patching for the anticipated life of the system; software must be on GSA's Enterprise Architecture IT Standards List.

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

Control ID	Control Title	Baseline	GSA Implementation Guidance
SC-8/ SC-8(1)	Transmission Confidentiality and Integrity Transmission Confidentiality and Integrity | Cryptographic Protection	M, H	Implemented encryption algorithms and cryptographic modules shall be FIPS-approved and FIPS PUB 140-2 validated, respectively. ○ Digital signature encryption algorithms ○ Block cypher encryption algorithms ○ Secure hashing algorithms For web services connections, implement end to end encryption terminating the connection at the web server; connections terminated at a load balancer shall employ re-encryption techniques to ensure end to end encryption. Internet accessible Websites shall implement HTTPS Only with HTTP Strict Transport Security (HSTS), have no weak ciphers, have no weak protocols, and preload .gov domains. (see Binding Operational Directive (BOD) 18-01, Enhance Email and Web Security). SSL/TLS implementations shall align with GSA IT Security Procedural Guide 14-69, *"SSL/TLS Implementation."*
SC-13	Cryptographic Protection	L, M, H	Implemented encryption algorithms and cryptographic modules shall be FIPS-approved and FIPS PUB 140-2 validated, respectively. ○ Digital signature encryption algorithms ○ Block cypher encryption algorithms ○ Secure hashing algorithms
SC-17	Public Key Infrastructure Certificates	M, H	Implement appropriate creation, use, and signing of crypto certs in agreement with GSA IT Security Procedural Guide 14-69, *"SSL/TLS Implementation,"* and NIST Special Publications 800-52, Revision 2 and 1800-16.
SC-18	Mobile Code	M, H	Systems must adhere to GSA's requirements regarding IT Standards and CIO-IT Security-07-35, "*Web Application Security*" and CIO-IT Security-17-81, "*Web Browser Technologies Hardening*," as applicable, to ensure only approved code (including mobile code) is used.
SC-22	Architecture and Provisioning for Name / Address Resolution Service	L, M, H	Information systems shall be Domain Name System Security Extensions (DNSSEC) compliant. Reference OMB Memorandum M-08-23, which requires all Federal Government departments and agencies that have registered and are operating second level .gov to be DNSSEC.

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

Control ID	Control Title	Baseline	GSA Implementation Guidance
SC-28 (1)	Protection of Information at Rest | Cryptographic Protection	L, M, H	**Systems that process Personally Identifiable Information (PII), Payment Card Industry (PCI) data, Authenticators (e.g., passwords, tokens, keys, certificates, hashes, etc.), and other sensitive data as determined by the AO, shall encrypt that data everywhere (i.e., at file level, database level, at rest, and in transit (see SC-8(1)). For databases, encryption of the whole database, table, column, or field levels is acceptable, as appropriate. Other methods including, but not limited to, application encryption or tokenization is also acceptable. For web services connections, implement end to end encryption terminating the connection at the web server; connections terminated at a load balancer shall employ re-encryption techniques to ensure end to end encryption.** Encryption algorithms shall be FIPS-approved with FIPS-validated encryption modules.
SI-2	Flaw Remediation	L, M, H	All projects and systems must be adequately tested for flaws; all Critical, High, and Moderate risk findings must be remediated prior to go-live. Post go-live, critical/very high vulnerabilities for Internet-accessible IP addresses must be remediated within 15 days, for all other assets critical/very high vulnerabilities must be remediated within 30 days; High vulnerabilities must be remediated within 30 days; Moderate vulnerabilities must be remediated within 90 days.
SI-3	Malicious Code Protection	L, M, H	All internal information systems must incorporate Bit9 and FireEye HX agents on supported operating systems. These agents will be provided.
SI-4	System Monitoring	L, M, H	All information systems must be monitored internally and across ingress/egress points for potentially malicious activity. In addition, all internal information systems must incorporate Bit9 and FireEye HX agents on supported operating systems. These agents will be provided.
SI-10	Information Input Validation	M, H	All systems accepting input from end users must validate the input in accordance with industry best practices and published guidelines, including GSA IT Security Procedural Guide 07-35, *"Web Application Security,"* and OWASP Top 10 Web Application Security Vulnerabilities.
SR-2	Supply Chain Risk Management Plan	L, M, H	Tier 3 (Information System) plans for each system should be developed consistent with the template in Appendix E of NIST SP 800-161.

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

Control ID	Control Title	Baseline	GSA Implementation Guidance
SR-6	Supplier Assessment and Reviews	M, H	
PM-21	Accounting of Disclosures	See note below	Requires accounting of disclosures of PII.
PM-25	Minimization of Personally Identifiable Information Used in Testing, Training, and Research	See note below	Requires implementation of policies and procedures to minimize PII used in testing, training, and research.
PT-5	Privacy Notice	See note below	Privacy notices help inform individuals about how their personally identifiable information is being processed by the system or organization
PT-5 (2)	Privacy Notice | Privacy Act Statements	See note below	Include Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.
PT-6	System of Records Notice	See note below	Federal agencies must publish a system of records notice in the Federal Register upon the establishment and/or modification of a Privacy Act system of record
PT-7 (1)	Specific Categories of Personally Identifiable Information | Social Security Numbers	See note below	Federal law and policy establish specific requirements for organizations' processing of Social Security numbers; organizations take steps to eliminate unnecessary uses of Social Security numbers and other sensitive information, and observe any particular requirements that apply.
RA-8	Privacy Impact Assessments	See note below	Conduct privacy impact assessments for systems, programs, or other activities before developing or procuring information technology that will process PII or before initiating a new collection of PII
SI-12 (1)	Information Management and Retention | Limit Personally Identifiable Information Elements	See note below	Limit personally identifiable information being processed in the information life cycle to specified elements.

Note: Privacy controls are not associated with a baseline. Controls are applicable/not applicable based on PII data being collected, stored, or transmitted.

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

3.4 Assessment and Authorization (A&A) Activities

The implementation of a new Federal Government IT system requires a formal approval process known as Assessment and Authorization (A&A). NIST Special Publication 800-37, Revision 2 (hereafter described as NIST 800-37) and GSA IT Security Procedural Guide 06-30, "*Managing Enterprise Cybersecurity Risk,"* provide guidelines for performing the A&A process. The system/application must have a valid assessment and authorization, known as an Authorization to Operate (ATO) (signed by the Federal government) before going into operation and processing GSA information. The failure to obtain and maintain a valid ATO will result in the termination of the contract. The system must have a new A&A conducted (signed by the Federal government) when significant changes are made to the system, and as specified in GSA IT Security Procedural Guide 06-30, "*Managing Enterprise Cybersecurity Risk,*" and the guides for GSA's other A&A processes referenced therein.

Assessing the System

1. The Contractor shall comply with Assessment and Authorization (A&A) requirements as mandated by Federal laws and policies, including making available any documentation, physical access, and logical access needed to support this requirement. The Level of Effort for the A&A is based on the System's NIST Federal Information Processing Standard (FIPS) Publication 199 categorization. Documents that contain CUI must be marked as such. Not all deliverables contain CUI. When in question, the contractor should use the NARA CUI Registry to help determine the appropriate designation for marking, handling or transmitting. The contractor shall create, maintain and update the following A&A documentation:
    - System Security and Privacy Plan (SSPP) completed in agreement with NIST Special Publication 800-18, Revision 1, *"Guide for Developing Security Plans for Federal Information Systems,"* and completed in accordance with GSA SSPP requirements and templates. The SSPP shall include as appendices required policies and procedures across 19 control families mandated per FIPS PUB 200, Rules of Behavior, and Interconnection Security Agreements (in agreement with NIST Special Publication 800-47, *"Security Guide for Interconnecting Information Technology Systems"*). The SSPP shall include; as an appendix, a completed GSA Control Tailoring Workbook (CTW) identified in Appendix A of this guide. The column in the CTW titled "Vendor/Contractor Defined Values" shall be used to document all contractor implemented parameter settings that differ from the GSA Defined Value and the Vendor/Contractor defined value when the value is deferred to the Vendor/Contractor. GSA's approval will be documented in the CTW column titled "GSA Approval of Vendor/Contractor Defined Values."
    - Contingency Plan completed in agreement with NIST Special Publication 800-34 and GSA IT Security Procedural Guide 06-29, "*Contingency Planning."*
    - Business Impact Analysis completed in agreement with NIST Special Publication 800-34 and GSA IT Security Procedural Guide 06-29, "*Contingency Planning."*

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

- Contingency Plan Test Report completed in agreement with GSA IT Security Procedural Guide 06-29, *"Contingency Planning."*
- Plan of Action & Milestones completed in agreement with GSA IT Security Procedural Guide 09-44, *"Plan of Action and Milestones (POA&M)."*
- Penetration Test Reports documenting the results of vulnerability analysis and exploitability of identified vulnerabilities. Note: Penetration testing is required for all Internet accessible, all FIPS 199 High, and all High Value Asset (HVA) information systems. These systems are required to complete an independent penetration test and provide an Independent Penetration Test Report documenting the results of the exercise as part of the A&A package. Reference GSA IT Security Procedural Guide 06-30, *"Managing Enterprise Cybersecurity Risk"* and GSA IT Security Procedural Guide 11-51, *"Conducting Penetration Test Exercises"* for penetration testing guidance.

2. Information systems must be assessed and authorized every three (3) years or whenever there is a significant change to the system's security posture in accordance with NIST Special Publication 800-37 Revision 2, "*Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy,*" and GSA IT Security Procedural Guide 06-30, "*Managing Enterprise Cybersecurity Risk*" or via continuous monitoring based on GSA IT Security Procedural Guide 12-66, "*Information Security Continuous Monitoring (ISCM) Strategy & Ongoing Authorization (OA) Program*" that is reviewed and accepted by the GSA CISO.
3. At the Moderate impact level and higher, the **<SELECT: contractor or Government>** is responsible for providing an independent Security Assessment/Risk Assessment in accordance with GSA IT Security Procedural Guide 06-30, *"Managing Enterprise Cybersecurity Risk*."
4. If the Government is responsible for providing a Security Assessment/Risk Assessment and Penetration Test, the Contractor shall allow GSA employees (or GSA designated third party contractors) to conduct A&A activities to include control reviews in accordance with NIST 800-53/NIST 800-53A and GSA IT Security Procedural Guide 06-30, *"Managing Enterprise Cybersecurity Risk*." Review activities include but are not limited to operating system vulnerability scanning, web application scanning, and database scanning of applicable systems that support the processing, transportation, storage, or security of GSA information. This includes the general support system infrastructure.
5. Identified gaps between required NIST 800-53 controls and the contractor's implementation as documented in the Security Assessment/Risk Assessment report shall be tracked for mitigation in a Plan of Action and Milestones (POA&M) document completed in accordance with GSA IT Security Procedural Guide 09-44, *"Plan of Action and Milestones (POA&M)."* Depending on the severity of the gaps, the Government may require them to be remediated before an Authorization to Operate is issued.
6. The Contractor is responsible for mitigating all security risks found during the A&A and continuous monitoring activities. Vulnerabilities must be mitigated as follows:

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

(1) For Internet-accessible IP addresses
   (a) Any Critical (Very High) scan vulnerabilities must be remediated within 15 days.
   (b) Any High scan vulnerabilities must be remediated within 30 days.
   (c) Any Moderate scan vulnerabilities must be remediated within 90 days.
(2) For all other assets
   (a) Any Critical (Very High) and High scan vulnerabilities must be remediated within 30 days.
   (b) Any Moderate scan vulnerabilities must be remediated within 90 days.

7. The Government will determine the risk rating of vulnerabilities.

Authorization of the System

1. Upon receipt of the documentation (A&A Package) described in GSA IT Security Procedural Guide 06-30, *"Managing Enterprise Cybersecurity Risk."* and NIST Special Publication 800-37 as documented above, the GSA Authorizing Official (AO) for the system (in coordination with the GSA Chief Information Security Officer (CISO), System Owner, Information System Security Manager (ISSM), and Information System Security Officer (ISSO)) will render an authorization decision to:
   - Authorize system operation w/out any restrictions or limitations on its operation;
   - Authorize system operation w/ restriction or limitation on its operation, or
   - Not authorize for operation.
2. The System Owner, AO, and supporting stakeholders including but not limited to System Custodians, supporting contractors, etc., shall make appropriate personnel available for interviews and provide documentation to the Federal Government, or their designee acting as their agent, in order to verify compliance with the requirements of GSA's Information Technology security program.

3.5 Reporting and Continuous Monitoring

Maintenance of the security authorization to operate will be through continuous monitoring of security controls of the contractor's system and its environment of operation to determine if the security controls in the information system continue to be effective over time in light of changes that occur in the system and environment. Through continuous monitoring, security controls and supporting deliverables are updated and submitted to GSA per the schedules below. The submitted deliverables (or lack thereof) provide a current understanding of the security state and risk posture of the information systems. They allow GSA AOs to make credible risk-based decisions regarding the continued operations of the information systems and initiate appropriate responses as needed when changes occur.

Deliverables to be provided Quarterly to the GSA ISSO, ISSM, and/or COR

1. Plan of Action & Milestones (POA&M) Update

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

Reference: NIST 800-53 control CA-5
Provide POA&M updates in accordance with requirements and the schedule set forth in GSA CIO IT Security Procedural Guide 09-44, "*Plan of Action and Milestones (POA&M).*"

Deliverables to be provided Annually or when there is a major change to the GSA ISSO, ISSM, and/or COR

1. Updated A&A documentation including the System Security and Privacy Plan, Contingency Plan. and Business Impact Analysis
    a. System Security and Privacy Plan
    Reference: NIST 800-53 control PL-2
    Review and update the System Security and Privacy Plan annually to ensure the plan is current and accurately describes implemented system controls and reflects changes to the contractor system and its environment of operation. The System Security and Privacy Plan must be in accordance with NIST 800-18, Revision 1, *"Guide for Developing Security Plans for Federal Information Systems."*
    b. Contingency Plan
    Reference: NIST 800-53 control CP-2
    Provide an annual update to the contingency plan completed in accordance with NIST 800-34, *"Contingency Planning Guide for Federal Information Systems"* and GSA IT Security Procedural Guide 06-29, "*Contingency Planning."*
    c. Business Impact Analysis
    Reference: NIST 800-53 control CP-2
    Provide an annual update to the business impact analysis completed in accordance with NIST 800-34, *"Contingency Planning Guide for Federal Information Systems"*, and GSA IT Security Procedural Guide 06-29, *"Contingency Planning."*
2. User Certification/Authorization Review Documents
    Reference: NIST 800-53 control AC-2
    Provide the results of the annual review and validation of system users' accounts to ensure the continued need for system access. The user certification and authorization documents will illustrate the organization establishes, activates, modifies, reviews, disables, and removes information system accounts in accordance with documented account management procedures.
3. Annual FISMA Self-Assessment
    Reference: NIST 800-53 control CA-2
    Deliver the results of the annual FISMA self-assessment conducted per GSA IT Security Procedural Guide 04-26, "*Federal Information Security Modernization Act (FISMA) Implementation."* Based on the controls selected for self-assessment, the GSA OCISO will provide the appropriate test cases for completion.
4. System Configuration Settings
    Reference: NIST 800-53 control CM-6

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

Establish and document mandatory configuration settings for information technology products employed within the information system that reflect the most restrictive mode consistent with operational requirements. Configuration settings are the configurable security-related parameters of information technology products that compose the information system. Systems shall implement GSA benchmarks for system hardening. GSA benchmarks may be exceeded but not lowered. Where a GSA benchmark does NOT exist, GSA technical guidelines, NIST guidelines, Center for Internet Security guidelines (Level 1), or industry best practice guidelines, as reviewed and accepted by the GSA AO.

All workstations and servers connected to the GSA network integrate with BigFix and have agents installed. Provide the most recent operating system Configuration Settings Compliance scan report.

5. Configuration Management Plan
   Reference: NIST 800-53 control CM-9
   Provide an annual update to the Configuration Management Plan for the information system.

6. Contingency Plan Test Report
   Reference: NIST 800-53 control CP-4
   Provide a contingency plan test report completed in accordance with GSA IT Security Procedural Guide 06-29, *"Contingency Planning."* A continuity test shall be conducted annually prior to mid-July of each year. The continuity test can be a tabletop test while the system is at the FIPS PUB 199 Low Impact level. The tabletop test must include Federal and hosting Contractor representatives. Functional exercises must be completed once every three years for FIPS PUB 199 Moderate impact systems and annually for FIPS PUB 199 High impact systems.

7. Incident Response Test Report
   Reference: NIST 800-53 control IR-3
   Provide an incident response plan test report documenting results of incident reporting process per GSA IT Security Procedural Guide 01-02, *"Incident Response*."

8. Information Exchanges (if applicable)
   Reference: NIST 800-53 control CA-3
   Systems with interconnections shall provide Interconnection Security Agreements (ISA) and supporting Memoranda of Agreement/Understanding (MOA/U), completed in accordance with NIST 800-47, *"Security Guide for Connecting Information Technology Systems,"* for existing and new interconnections. Per NIST 800-47, an interconnection is the direct connection of two or more IT systems for the purpose of sharing data and other information resources through a pipe, such as ISDN, T1, T3, DS3, VPN, etc. ISAs shall be submitted as appendices as part of the annual System Security and Privacy Plan submission. ISAs shall include, if applicable, any changes since the last submission; updated ISAs are required at least every three years.

9. Penetration Testing Report
   Reference: NIST 800-53 control CA-8

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

All Internet accessible systems, and all FIPS PUB 199 High impact systems are required to complete an independent penetration test and provide a Penetration Test Report documenting the results of the exercise as part of their A&A package. Annual penetration tests are required for these same systems in accordance with GSA Order CIO 2100.1 and CIO-IT Security-11-51, "*Conducting Penetration Test Exercises.*"

10. Personnel Screening and Security
    Reference: NIST 800-53 control PS-3, NIST 800-53 control PS-7
    Furnish documentation reflecting favorable adjudication of background investigations for all personnel (including subcontractors) supporting the system. Contractors shall comply with GSA Order CIO 2100.1, "*GSA Information Technology (IT) Security Policy"* and GSA Order ADM 2181.1, "*Homeland Security Presidential Directive-12, Personal Identity Verification and Credentialing, and Background Investigations for Contractors."* GSA separates the risk levels for personnel working on Federal computer systems as follows:

    - A favorable initial fitness/suitability determination must be granted and a Tier 1 or higher background investigation initiated before access to the GSA network or any GSA IT system. There shall be no waivers to this requirement for GSA network and IT system access for GSA employees or contractors.
    - A favorable initial fitness/suitability determination must be granted and a Tier 2 or higher background investigation initiated before access to PII/CUI is granted. The authority and access shall be determined by the appropriate GSA Supervisor (for GSA employees) or CO (for contract personnel), Data Owner, and the System's AO. Each System's AO, with the request of the GSA Supervisor, Data Owner or CO, shall evaluate the risks associated with each such request.
    - A favorable suitability determination must be completed at a Tier 2 or higher background investigation before privileged access to the GSA network or IT systems is granted. A waiver may be requested in order to maintain GSA business operations; however such requests should be used judiciously and not incur unnecessary risks to GSA.

    If final adjudication of a background investigation is unfavorable, GSA network and IT system access must be revoked, and any GFE, including the GSA PIV card, must be retrieved and returned to OMA.

3.6 GSA Privacy Requirements

Personally identifiable information (PII) **<SELECT: is or is not>** in the scope of the acquisition and PII **<SELECT: is or is not>** expected to be stored, processed, or transmitted in the vendor's information system. The collection, maintenance or dissemination of any PII that is subject to the Privacy Act and/or the E-Government Act will be handled in full accordance with all GSA rules of conduct and in accordance with GSA Privacy Program requirements.

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

The contractor shall work with GSA to prepare a Privacy Threshold Assessment (PTA) to confirm and document PII is not in scope, or to determine which categories of information will be stored, processed, or transmitted by the system. The PTA must be completed before development begins and whenever a change with a privacy impact (e.g., a new category of information is collected) is made to an existing system. PTAs are required as part of GSA's process to determine whether a Privacy Impact Assessment (PIA) and/or a System of Records Notice (SORN) is required, and if any other privacy requirements apply to the information system. Information regarding PIAs can be found in this GSA Policy.

PII (should it come into scope) will require the following guidelines be adhered to.

- The vendor's information system must be authorized at least at the FIPS PUB 199 Moderate level.
- For any system that collects, maintains or disseminates PII, a PIA must be completed by the contractor and provided to the GSA Privacy Office for review along with the other authorization to operate (ATO) documents.
- If the system retrieves information using PII, the Privacy Act applies and it must have a system of records notice (SORN) published in the Federal Register.
- If PII is collected from individuals by the system, a Privacy Act Statement (i.e., Privacy Notice) must be provided to users prior to their use of the application on what data is being collected and why, as well as the authority for the collection and the impact of not providing some or all of it. The Privacy Act Statement must be available to the individual directly on the form used to collect the information. Providing a link back to the Statement from the form is acceptable.

Per OMB A-130 Privacy Act Statements must include:

(1) the authority (whether granted by statute or executive order) that authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary;
(2) the principal purpose(s) for which the information is intended to be used;
(3) the published routine uses to which the information is subject;
(4) the effects on the individual, if any, of not providing all or any part of the requested information; and
(5) an appropriate citation (and, if practicable, a link) to the relevant SORN(s).

An example Privacy Act Statement is available at GSA's Privacy Act Statement for Design Research.

Note: Systems that access data a user creates must assume a user may include privacy data/PII in the system unless the data creation is restricted to data controlled by the system.

All contractor staff who have significant privacy information responsibilities must complete GSA's mandatory privacy awareness and role-based training courses. This includes contractors

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

who work with PII as part of their work duties (e.g., Human Resource staff, Finance staff, and managers/supervisors).

3.7 Additional Stipulations

1. When containing sensitive information, deliverables shall be labeled Controlled Unclassified Information (CUI) or contractor selected designation per document sensitivity. Not all deliverables contain CUI. When in question, the contractor should use the National Archives and Records Administration (NARA) CUI Registry to help determine the appropriate designation for marking. External transmission/dissemination of CUI to or from a Government computer must be encrypted. Certified encryption modules must be used in accordance with FIPS PUB 140-2, *"Security Requirements for Cryptographic Modules."*
2. The Contractor shall certify applications are fully functional and operate correctly as intended on systems using benchmarks from GSA technical guidelines, NIST guidelines, Center for Internet Security guidelines, or industry best practice guidelines, as reviewed and accepted by the GSA AO. The standard installation, operation, maintenance, update, and/or patching of software shall not alter the configuration settings from the approved benchmark configuration. Information technology for Windows systems should use the Windows Installer Service for installation to the default "program files" directory and should be able to silently install and uninstall. Applications designed for normal end users shall run in the standard user context without elevated system administration privileges. The contractor shall use tools to verify their products operate correctly with the approved benchmark configurations and do not alter the benchmark settings.
3. The Contractor shall cooperate in good faith in defining non-disclosure agreements (NDAs) that other third parties must sign when acting as the Federal government's agent.

Note: GSA's Office of the General Counsel (OGC) is available to coordinate on defining NDA requirements. Upon request, GSA OGC can advise on NDA development.

4. The Government has the right to perform manual or automated audits, scans, reviews, or other inspections of the IT environment being used to provide or facilitate services for the Government. The Contractor shall be responsible for the following privacy and security safeguards:
    a. The Contractor shall not publish or disclose in any manner, without the Contracting Officer's written consent, the details of any safeguards either designed or developed by the Contractor under this contract or otherwise provided by the Government. Exception - Disclosure to a Consumer Agency for purposes of A&A verification or to the MAX.Gov portal. To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data, the Contractor shall afford the Government access to facilities, installations, technical capabilities,

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

operations, documentation, records, and databases used to provide or facilitate services for the Government within 72 hours of the request. Access to support incident investigations, shall be provided as soon as possible but not longer than 72 hours after request.

The program of inspection shall include, but is not limited to:

- Authenticated and unauthenticated operating system/network vulnerability scans.
- Authenticated and unauthenticated web application vulnerability scans
- Automated scans can be performed by Government personnel, or agents acting on behalf of the Government, using Government operated equipment, and Government specified tools. If the vendor chooses to run its own automated scans or audits, results from these scans may at the Government's discretion, be accepted in lieu of Government performed vulnerability scans. In these cases, scanning tools and their configuration shall be approved by the Government. In addition, the results of vendor-conducted scans shall be provided in full to the Government.

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

5. The Contractor shall comply with Section 1634 of Public Law 115-91 that prohibits use of any hardware, software, or services developed or provided, in whole or in part, by— (1) Kaspersky Lab (or any successor entity); (2) any entity that controls, is controlled by, or is under common control with Kaspersky Lab; or (3) any entity of which Kaspersky Lab has majority ownership.

6. The Contractor shall comply with 52.204-25 of the Federal Acquisition Regulation (FAR). It prohibits, under Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232), contractors from providing to the Government any equipment, system, or service that uses telecommunications equipment or video surveillance services from certain named companies as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception or waiver is granted per the FAR. It also prohibits, under Section 889(a)(1)(B), contractors from using any equipment, system, or service that uses telecommunications or video surveillance equipment or services from certain named companies as a substantial or essential component of any system or as critical technology as part of any system, unless an exception or waiver is granted per the FAR. The proscribed companies are Huawei Technologies Company, ZTE Corporation, Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, and Dahua Technology Company and their subsidiaries and affiliates.

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

4 Low Impact Software as a Service (LiSaaS) – IT Security and Privacy Requirements

To be considered for award, the contractor must comply with GSA IT's Low-Impact SaaS (LiSaaS) review. The successful vendor will need to ensure any software-as-a-service provided under this contract meets GSA security and privacy requirements prior to invoicing the government for services received under this contract. This includes working with GSA to ensure the Software-as-a-Service (SaaS) passes the current Low-impact-software-as-a-service (LiSaaS) approval process, as outlined in GSA IT Security Procedural Guide 16-75, "*Low Impact Software as a Service (SaaS) Solutions Authorization Process*."

4.1 Assessment of the System

The contractor shall provide evidence in support of meeting the requirements for the review activities stated in GSA IT Security Procedural Guide 16-75, "*Low Impact Software as a Service (SaaS) Solutions Authorization Process*," and as summarized below. As stated in the guide items (2)-(6) in the list below, may be satisfied by a letter of attestation submitted by the Office of the Chief Security Officer ISSO Support Division (IST) Director or designee, based on a demonstration and review of artifacts. A checklist template will be provided to the contractor, as applicable.

(1) Completion of a LiSaaS Solution Review Checklist Template (including supporting artifacts). This checklist provides a summary of the service function and purpose provided by the LiSaaS solution. It includes the who, what, when, where, and how of the solution, including any leveraged infrastructures and SaaS integrations, as applicable. Instructions are contained in the template. In the process of completing the checklist solutions deemed to be very low/negligible risk will have a LiSaaS Solutions Profile completed by GSA support personnel.

(2) Document how system and security parameters deferred to customers are implemented. Do not use the vendor-supplied defaults for system passwords and other security parameters. GSA security policies and best practices should be used to the greatest extent possible.

(3) Submit latest web application scan results (e.g., NetSparker, Acunetix, Burp Suite Pro, etc.). The OCISO can assist with web application scans if the vendor(s) do not have an in house web application scanning capability.

(4) Submit latest operating system (OS) vulnerability scan results (e.g., Tenable Nessus, Qualys, nCircle, McAfee Vulnerability Manager, etc.). Reference NIST SP 800-53 control RA-5 – Vulnerability Monitoring and Scanning.

   a. Vendors that are Payment Card Industry Data Security Standard (PCI DSS) compliant or have the McAfee Secure Seal or TrustGuard Seal may provide the results of their latest PCI DSS Compliant, McAfee Secure Seal or TrustGuard quarterly scan.

   b. Vendors that do not meet the PCI DSS, McAfee, or TrustGuard standards listed, must provide their most recent OS vulnerability scan results.

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

(5) An acceptable flaw remediation process. Vendors must be able to identify and remediate information system flaws in a timely manner.
(6) Results of one of the following audits/certifications:
- Service Organization Control (SOC) 2/Statements on Standards for Attestation Engagements (SSAE) 18
- SysTrust/WebTrust
- ISO/IEC 27001
- Payment Card Industry Data Security Standard (PCI DSS)

Note: Although the minimum requirement is for the SSAE/SOC 2 audit report or one of the vendor certifications; the GSA AO and the CISO will take a holistic view of the application based on all of the documentation presented to determine the overall risk of the application as well as any residual risks that may need to be accepted when considering the application for use. If the documentation presented does not provide an adequate understanding of the systems security posture and/or is deemed insufficient to make a risk determination; additional information will be required.

4.2 Authorization of the System

The authorization process supports an ATO valid for:

- No more than one year if the application is determined to be Low Risk based on the evidence provided.
- Up to three years if the application is determined to be a commodity ancillary service that presents Very Low/Negligible Risk based on the evidence provided.

If not already FedRAMP authorized, any application granted a one-year ATO must obtain a FedRAMP tailored authorization within one year of its ATO. If, within three months of receiving its one-year ATO, progress towards a FedRAMP Tailored authorization has not been observed, GSA will start to cease engagement with the vendor and pursue alternative solutions. For detailed requirements of a FEDRAMP Tailored authorization visit the FEDRAMP Tailored for Low-Impact Software-as-a-Service (LI-SaaS) page. Without a LiSaaS approval, GSA will not be able to use the software for the base year of the contract, and without FedRAMP approval, GSA will be unable to use the product for the option years of the contract.

The contractor's agreement to the LiSaaS and FedRAMP requirements are required. If the contractor does not agree, no contract award will be made.

If at any time, the vendor is either unwilling or unable to meet any of the process requirements, GSA may choose to cancel the contract and terminate any outstanding orders.

4.3 Maintenance of ATO and Continuous Monitoring

The LiSaaS ATO will be contingent on annual validation of the requirements identified in Section 4.1, including:

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

- The latest SSAE/SOC 2 audit report, vendor certification, or PCI DSS compliance;
- Annual web application vulnerability scan results;
- Most recent quarterly operating system vulnerability scan results or proof of compliance with PCI DSS, McAfee Secure Seal, or TrustGuard standards/seals;
- Annual recertification that GSA is still using the service.

Note: If an attestation letter was used to validate any of the requirements listed above for the existing ATO, then a new attestation letter or the artifact/deliverables listed must be provided.

If at any time, the vendor is either unwilling or unable to meet any of the requirements, the ATO shall be terminated upon approval of the AO. It is the responsibility of the assigned ISSO to ensure the requirements continue to be met. Significant changes shall be reported to the ISSM, who with the ISSO manages the A&A package.

The vendor shall report if its audit report/certification renews or expires and if any of the other required activities cannot be supported.

4.4 Protection of Information

The contractor shall be responsible for properly protecting all information used, gathered, disclosed, or developed as a result of work under this contract. The contractor shall also protect all Government data, etc. by treating the information as sensitive. All information gathered or created under this contract should be considered as confidential information. It is anticipated that this information will be gathered, created and stored within the primary work location. If contractor personnel must remove any information from the primary work area they should protect it to the same extent they would their proprietary data and/or company trade secrets. The use of any information that is subject to the Privacy Act will be utilized in full accordance with all rules of conduct as applicable to Privacy Act Information. Personnel shall adhere to the Privacy Act, Title 5 of the U. S. Code, Section 552a and applicable agency rules and regulations.

4.5 Data Ownership and Unrestricted Rights to Data

All Government data collected in the system is the property of the Federal Government. The Government will retain unrestricted rights to government data. The ordering activity retains All data collected by the system shall be provided by the Contractor (system provider) as requested during the contract period and at the completion of the contract period.

Government data rights of software deliverables shall be in accordance with FAR 52. 227-19 Commercial Computer Software License and/or FAR 52. 227-14 Rights in Data - General. Ownership of data entered into any and all systems, system documentation, all deliverables produced in the performance of this contract, and other related system information shall reside with the Government.

The Contractor shall place the following copyright notice on all materials, documents, deliverables, etc. developed during the performance of this contract:

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

For purposes of clarity, the intent of the government is for intellectual property to be vested in the federal government for work paid for by the federal government. All documents, graphics, and code created under this contract are the intellectual property of the federal government including, but not limited to, plans, reports, schedules, software code, software designs, graphics, etc. In the event that the federal government implements under this contract open-source software and pays for the cost of the implementation of open-source software, the final changes and edits to the code and configuration (such as work to integrate plug-ins) are the intellectual property of the federal government.

4.6 Personally Identifiable Information

Personally identifiable information (PII) data **is not** in the scope of the acquisition and PII data **is not** expected to be stored in the vendor's SaaS solution. The contractor shall work with GSA to prepare a Privacy Threshold Assessment (PTA) to either document PII is not in scope, or determine which categories of information will be stored, processed, or transmitted by the system. The use of any information that is subject to the Privacy Act will be utilized in full accordance with all rules of conduct as applicable to Privacy Act Information.

Privacy data (should it come into scope) will require that the vendor’s SaaS solution be FedRAMP authorized at least at the FIPS PUB 199 Moderate level.

4.7 Data Availability

The data must be available to the Government upon request within one business day or within the timeframe negotiated with the Contractor, and shall not be used for any other purpose other than that specified herein. The contractor shall provide requested data at no additional cost to the government.

4.8 Data Release

Contractor will not disclose Customer Data to any government or third party or access or use Customer Data; except in each case as necessary to maintain the SaaS solution or to provide the SaaS solution to Customer in accordance with this contract, or as necessary to comply with the law or a valid and binding order of a governmental or regulatory body (such as a subpoena or court order). Unless it would be in violation of a court order or other legal requirement, the Contractor will give the Government reasonable notice of any such legal requirement or order, to allow the Government to seek a protective order or other appropriate remedy.

4.9 Confidentiality and Nondisclosure

Personnel (contractor/subcontractor employee) working on any of the described tasks, may at Government request, be required to sign formal non-disclosure and/or conflict of interest agreements (NDA/CUI) to guarantee the protection and integrity of Government information and documents. The Contractor shall submit to the COR a completed confidentiality and NDA

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

form for each individual contractor/subcontractor.

Additionally, any information made available to the Contractor by the Government shall be used only for the purpose of carrying out the provisions of this contract and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of the contract. In performance of this contract, the Contractor assumes responsibility for protection of the confidentiality of Government records and shall ensure that all work performed by its subcontractors shall be under the supervision of the Contractor or the Contractor's responsible employees. Each officer or employee of the Contractor or any of its subcontractors to whom any Government record may be made available or disclosed shall be notified in writing by the Contractor that information disclosed to such officer or employee can be used only for that purpose and to the extent authorized herein. Further disclosure of any such information, by any means, for a purpose or to an extent unauthorized herein, may subject the offender to criminal sanctions imposed by 18 U. S. C. §§ 1030.

Note: GSA's Office of the General Counsel (OGC) is available to coordinate on defining NDA requirements. Upon request GSA OGC can advise on NDA development.

4.10 Section 508 Compliance

The Contractor(s) shall provide accessibility based on Section 508 of the Rehabilitation Act of 1973 (29 U. S. C. 794d). All information and communication technology (ICT) delivered must meet the applicable revised accessibility standards at 36 CFR 1194, unless an agency exception to this requirement exists. The 36 CFR 1194 implements Section 508 of the Rehabilitation Act of 1973, as amended. All deliverables will be Section 508 compliant, and will be reviewed for compliance by the government which reserves the right to reject the deliverable(s) until remediation of deficiencies has been successfully completed by the Contractor. Complete technical descriptions are provided on the following website: http://www.section508.gov.

Where appropriate, the Contractor(s) shall indicate whether each product or service is compliant or noncompliant with the accessibility standards at 36 CFR 1194. Further, the quote must indicate where full details of compliance can be found (e. g., vendor product accessibility template/accessibility conformance report (VPAT/ACR), vendor's website or other exact location).

4.11 Additional Stipulations

1. When containing sensitive information, deliverables shall be labeled Controlled Unclassified Information (CUI) or contractor selected designation per document sensitivity. Not all deliverables contain CUI. When in question, the contractor should use the National Archives and Records Administration (NARA) CUI Registry to help determine the appropriate designation for marking. External transmission/dissemination of CUI to or from a Government computer must be encrypted. Certified encryption modules must be used in accordance with FIPS PUB 140-

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

2[6], "*Security Requirements for Cryptographic Modules*."

2. The contractor shall cooperate in good faith in defining NDAs that other third parties must sign when acting as the Federal government's agent.

Note: GSA's Office of the General Counsel (OGC) is available to coordinate on defining NDA requirements. Upon request GSA OGC can advise on NDA development.

3. The Government has the right to perform manual or automated audits, scans, reviews, or other inspections of the vendor's IT environment being used to provide or facilitate services for the Government. The Contractor shall be responsible for the following privacy and security safeguards:
    a. To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data, the Contractor shall afford the Government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases within 72 hours of the request. Access to support incident investigations, shall be provided as soon as possible but not longer than 72 hours after request.
    b. Physical Access Considerations – If the SaaS provider is operated within an IaaS that is FedRAMP authorized (e. g., AWS); physical access to the physical datacenter environment will be governed by the terms of access allowed by the underlying infrastructure provider as defined in the FedRAMP A&A authorization package.
    c. The program of inspection shall include, but is not limited to:
        - Authenticated and unauthenticated operating system/network vulnerability scans
        - Authenticated and unauthenticated web application vulnerability scans
        - Automated scans can be performed by Government personnel, or agents acting on behalf of the Government, using Government operated equipment, and Government specified tools. If the vendor chooses to run its own automated scans or audits, results from these scans may at the Government's discretion, be accepted in lieu of Government performed vulnerability scans. In these cases, scanning tools and their configuration shall be approved by the Government. In addition, the results of vendor-conducted scans shall be provided in full to the Government.
    d. If new or unanticipated threats or hazards are discovered by either the Government or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.

[6] NIST has issued FIPS 140-3, FIPS 140-2 modules are still being validated and will be accepted through September 22, 2026. For additional information see the NIST cryptographic module validation program webpage.

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

4. The Contractor shall comply with Section 1634 of Public Law 115-91 that prohibits use of any hardware, software, or services developed or provided, in whole or in part, by— (1) Kaspersky Lab (or any successor entity); (2) any entity that controls, is controlled by, or is under common control with Kaspersky Lab; or (3) any entity of which Kaspersky Lab has majority ownership.
5. The Contractor shall comply with 52.204-25 of the Federal Acquisition Regulation (FAR). It prohibits, under Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232), contractors from providing to the Government any equipment, system, or service that uses telecommunications equipment or video surveillance services from certain named companies as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception or waiver is granted per the FAR. It also prohibits, under Section 889(a)(1)(B), contractors from using any equipment, system, or service that uses telecommunications or video surveillance equipment or services from certain named companies as a substantial or essential component of any system or as critical technology as part of any system, unless an exception or waiver is granted per the FAR. The proscribed companies are Huawei Technologies Company, ZTE Corporation, Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, and Dahua Technology Company and their subsidiaries and affiliates.

4.12 Terms of Service

Many terms found in commercial ToS or End User License Agreements (EULA) are not acceptable when the Government is the end user. The Office of Chief Information Officer (OCIO) requires that software and services within the GSA Enterprise have approved ToS or EULA.

The Contractor's SaaS will undergo a formal review by GSA as part of the review/approval process. The Contractor's ToS shall be found to be acceptable to the government or a modified ToS negotiated as part of the approval review, prior to final authorization.

4.13 References

GSA IT Security Procedural Guide 16-75, "*Low Impact Software as a Service (LiSaaS) Solutions Authorization Process*"

FIPS PUB 199, *"Standards for Security Categorization of Federal Information and Information Systems"*

CSP Authorization Playbook-Getting Started with FedRAMP

5 Cloud Information Systems – IT Security and Privacy Requirements

The contractor shall implement the controls contained within the FedRAMP Cloud Computing Security Requirements Baseline and FedRAMP Continuous Monitoring Requirements for **<SELECT Low, Moderate, or High>** impact systems (as defined in FIPS PUB 199). These

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

documents define requirements for compliance to meet minimum Federal information security and privacy requirements for **<SELECT Low, Moderate, or High>** impact systems. The FedRAMP baseline controls are based on NIST Special Publication 800-53, Revision 4, *"Security and Privacy Controls for Information Systems and Organizations,"* and includes a set of additional controls for use within systems providing cloud services to the federal government. FedRAMP is in the process of planning its transition to Revision 5, once the transition is complete the controls in the table in Section 5.3 will be updated to reflect FedRAMP's transition.

The contractor shall generally, substantially, and in good faith follow FedRAMP guidelines and Security guidance. In situations where there are no procedural guides, the contractor shall use generally accepted industry best practices for IT security.

GSA may choose to cancel the contract and terminate any outstanding orders if the contractor has its FedRAMP authorization (Joint Authorization Board [JAB] Provisional or Agency) revoked and the deficiencies are greater than agency risk tolerance thresholds.

5.1 Assessment and Authorization

5.2 Assessment of the System

1. The contractor shall comply with FedRAMP requirements as mandated by Federal laws and policies, including making available any documentation, physical access, and logical access needed to support this requirement. The Level of Effort for the A&A is based on the System's FIPS PUB 199 categorization. The contractor shall create, maintain and update the following documentation using FedRAMP requirements and templates, which are available at FedRAMP.
    - Privacy Impact Assessment (PIA)
    - FedRAMP Test Procedures and Results
    - Security Assessment Report (SAR)
    - System Security Plan (SSP)
    - Contingency Plan (CP)
    - Business Impact Analysis
    - Contingency Plan (CP) Test Results
    - Plan of Action and Milestones (POA&M)
    - Continuous Monitoring Plan (CMP)
    - FedRAMP Control Tailoring Workbook
    - Control Implementation Summary Table
    - Results of Penetration Testing
    - Software Code Review
    - Interconnection Security Agreements/Service Level Agreements/Memorandum of Agreements
2. Information systems must be assessed by an accredited FedRAMP Third Party Assessment Organization (3PAO) initially and whenever there is a significant change to

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

the system's security posture in accordance with the FedRAMP Continuous Monitoring Plan.

3. The Government reserves the right to perform Security Assessment and Penetration Testing (of its instance). If the Government exercises this right, the contractor shall allow Government employees (or designated third parties) to conduct Security Assessment and Penetration Testing activities to include control reviews in accordance with FedRAMP requirements. Penetration shall be supported by mutually agreed upon Rules of Engagement (RoE). Review activities include but are not limited to manual penetration testing; automated scanning of operating systems, web applications; wireless scanning; network device scanning to include routers, switches, and firewall, and IDS/IPS; databases and other applicable systems, including general support structure, that support the processing, transportation, storage, or security of Government information for vulnerabilities.
4. The contractor shall provide access to the Federal Government, or their designee acting as their agent, when requested, in order to verify compliance with the requirements for an Information Technology security program. The Government reserves the right to conduct on-site inspections. The contractor shall make appropriate personnel available for interviews and provide all necessary documentation during this review.
5. Physical Access Considerations – If the Cloud Service Provider (CSP) is operated within an Infrastructure as a Service (IaaS) that is FedRAMP authorized (e.g., AWS); physical access to the physical datacenter environment will be governed by the terms of access allowed by the underlying infrastructure provider as defined in the FedRAMP A&A authorization package.
6. Identified gaps between required FedRAMP Security Control Baselines and Continuous Monitoring controls and the contractor's implementation as documented in the Security Assessment Report shall be tracked by the contractor for mitigation in a Plan of Action and Milestones (POA&M) document. Depending on the severity of the gaps, the Government may require them to be remediated before a GSA authorization is issued.
7. The contractor is responsible for mitigating all security risks found during A&A and continuous monitoring activities. All high-risk vulnerabilities must be mitigated within 30 days and all moderate risk vulnerabilities must be mitigated within 90 days from the date vulnerabilities are formally identified. The Government will determine the risk rating of vulnerabilities.

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

5.3 Authorization of the System

1. If the CSP Software as a Service (SaaS) or Platform as a Service (PaaS) is FedRAMP authorized (i.e., listed as FedRAMP authorized on the FedRAMP website:

   https://marketplace.fedramp.gov/index.html#/products?sort=productName&status=Compliant

   GSA will leverage the CSP's FedRAMP Assessment and Authorization package to document and assess the customer controls for which GSA has responsibility and issue a GSA ATO for the agency's instance of the CSP's SaaS or PaaS offering. The CSP shall work with the GSA to facilitate documentation and assessment of required customer controls, as necessary.

2. If the CSP SaaS or PaaS offering is NOT already FedRAMP authorized, it shall:

   a. Operate on an CSP IaaS environment that is FedRAMP authorized; AND

   b. Be listed as FedRAMP In Process on the FedRAMP Website - https://marketplace.fedramp.gov/index.html#/products?sort=productName&status=In%20Process

      OR be listed as FedRAMP Ready on the FedRAMP website - https://marketplace.fedramp.gov/index.html#/products?sort=productName&status=FedRAMP%20Ready

   c. Shall deliver within 90 days of contract award a FedRAMP Readiness Assessment Review completed by a FedRAMP 3PAO following the FedRAMP Readiness Assessment Guidelines. The FedRAMP Readiness Assessment Review demonstrates the CSPs overall readiness for FedRAMP authorization and whether it has a viable path to achieve a FedRAMP authorization within one (1) year of the contract award. If the CSP does not provide a FedRAMP Readiness Assessment as prescribed or the assessment demonstrates a significant gap in capabilities that will preclude achievement of a FedRAMP authorization within 1 year of the contract award, then, GSA will terminate the contract.

   If requirements a-c, as defined above, are met the CSP will have one (1) year from the date of contract award to achieve FedRAMP authorization. During this transitional period, GSA may issue an agency specific authorization (i.e., not FedRAMP) not to exceed one (1) year (to allow the CSP to achieve FedRAMP compliance) leveraging an existing ATO with another Federal Department/Agency (D/A) (with supporting A&A Package). The CSP may have a non-FedRAMP ATO with another D/A or be based on the GSA Moderate Impact SaaS Solutions process as described in GSA IT Security Procedural Guide 06-30, "*Managing Enterprise Cybersecurity Risk.*" The CSP shall make available any existing assessment and authorization package for GSA review and provide necessary documentation and access to facilitate the GSA Moderate Impact SaaS A&A process. Without a FedRAMP authorization within 1 year of contract award; GSA will not be able to use the product for the option years and shall terminate the contract.

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

3. CSP shall ensure these essential security controls are implemented. CSP shall implement FedRAMP control parameters and implementation guidance, as applicable. Further, the CSP shall make the proposed system and security architecture of the information system available to the Security Engineering Division, in the Office of the Chief Information Security Officer for review and approval before commencement of system build (architecture, infrastructure, and code (as applicable)) and/or the start as A&A activities.

Control ID	Control Title	FedRAMP Baseline
AC-2	Account Management	L, M, H
AU-2	Audit Events	L, M, H
CM-6	Configuration Settings	L, M, H
CP-7	Alternative Processing Site	M, H
CP-8	Telecom Services	M, H
IA-2 (1)	Identification and Authentication (Organizational Users) | Network Access to Privileged Accounts	L, M, H
IA-2 (2)	Identification and Authentication (Organizational Users) | Network Access to Non-Privileged Accounts	M, H
IA-2 (12)	Identification and Authentication (Organizational Users) | Acceptance of PIV Credentials	L, M, H
IA-7	Cryptographic Module Authentication	L, M, H
MP-4	Media Storage	M, H
MP-5	Media Transport	M, H
PL-8	Information Security Architecture	M, H
RA-5	Vulnerability Scanning	L, M, H
SC-8 / SC-8(1)	Transmission Confidentiality and Integrity / Transmission Confidentiality and Integrity | Cryptographic Protection	M, H
SC-13	Cryptographic Protection	L, M, H
SC-17	Public Key Infrastructure Certificates	M, H
SC-18	Mobile Code	M, H
SC-22	Architecture and Provisioning for Name / Address Resolution Service	L, M, H
SC-28 (1)	Protection of Information at Rest | Cryptographic Protection	M, H

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

Control ID	Control Title	FedRAMP Baseline
SI-2	Flaw Remediation	L, M, H
SI-3	Malicious Code Protection	L, M, H
SI-4	Information System Monitoring	L, M, H
SI-10	Information Input Validation	M, H

5.4 Reporting and Continuous Monitoring

Maintenance of the FedRAMP Authorization will be through continuous monitoring and periodic audit of the operational controls within a contractor's system, environment, and processes to determine if the security controls in the information system continue to be effective over time in light of changes that occur in the system and environment. Through continuous monitoring, security controls and supporting deliverables are updated in agreement with FedRAMP guidelines and submitted to the MAX.Gov Portal or repository designated by the FedRAMP program.

The submitted deliverables (or lack thereof) provide a current understanding of the security state and risk posture of the information systems. The deliverables will allow the Federal Departments/Agencies leveraging the services providers' cloud offering to make credible risk-based decisions regarding the continued operations of the information systems and initiate appropriate responses as needed when changes occur. Contractors will be required to provide updated deliverables and automated data feeds as defined in the FedRAMP Continuous Monitoring Plan.

The contractor shall provide continuous monitoring deliverables in support of a one (1) year conditional authorization (if necessary) to achieve FedRAMP authorization. Deliverables shall include:

- Quarterly OS-including database, and web application, vulnerability scans as specified in the NIST SP 800-53 Control RA-5 parameter in GSA's Control Tailoring Workbook (deliverable shall include raw results and findings shall be included in the POA&M document);
- Quarterly Plan of Action and Milestones (POA&M);
- Annual A&A Package updates including the System Security and Privacy Plan, Contingency Plan, Business Impact Analysis, Configuration Management Plan, Contingency Plan Test Report, and Annual FISMA Assessment.

Upon achievement of FedRAMP authorization, GSA will accept the FedRAMP A&A and continuous monitoring documentation made available on the MAX.Gov Portal or a repository designated by the FedRAMP program in agreement with FedRAMP guidelines to satisfy the continuous monitoring requirement.

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

5.5 Personnel Security Requirements

Contractor shall furnish documentation reflecting favorable adjudication of background investigations for all personnel (including subcontractors) supporting the system. Contractors shall comply with GSA Order CIO 2100.1, "*GSA Information Technology (IT) Security Policy,"* and GSA Order ADM 2181.1, "*Homeland Security Presidential Directive-12, Personal Identity Verification and Credentialing, and Background Investigations for Contractors."* GSA separates the risk levels for personnel working on Federal computer systems as follows:

- A favorable initial fitness/suitability determination must be granted and a Tier 1 or higher background investigation initiated before access to the GSA network or any GSA IT system. There shall be no waivers to this requirement for GSA network and IT system access for GSA employees or contractors.
- A favorable initial fitness/suitability determination must be granted and a Tier 2 or higher background investigation initiated before access to PII/CUI is granted. The authority and access shall be determined by the appropriate GSA Supervisor (for GSA employees) or CO (for contract personnel), Data Owner, and the System's AO. Each System's AO, with the request of the GSA Supervisor, Data Owner or CO, shall evaluate the risks associated with each such request.
- A favorable suitability determination must be completed at a Tier 2 or higher background investigation before privileged access to the GSA network or IT systems is granted. A waiver may be requested in order to maintain GSA business operations; however such requests should be used judiciously and not incur unnecessary risks to GSA.

If final adjudication of a background investigation is unfavorable, GSA network and IT system access must be revoked, and any GFE, including the GSA PIV card, must be retrieved and returned to OMA.

GSA shall sponsor the investigation when deemed necessary. No access shall be given to government computer information systems and government sensitive information without a background investigation being verified or in process. If results of background investigation are not acceptable, then access shall be terminated.

The Contractor shall provide a report of separated staff on a monthly basis, beginning 60 days after execution of the option period.

5.6 Sensitive Information Storage

Controlled Unclassified Information (CUI), data, and/or equipment will only be disclosed to authorized personnel on a need-to-know basis. The contractor shall ensure that appropriate administrative, technical, and physical safeguards are established to ensure the security and confidentiality of this information, data, and/or equipment is properly protected. When no longer required, this information, data, and/or equipment will be returned to Government control, destroyed, or held until otherwise directed. Destruction of items shall be accomplished by following NIST Special Publication 800-88, *"Guidelines for Media Sanitization."* The

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

destruction, purging or clearing of media specific to the CSP will be recorded and supplied upon request of the Government.

5.7 Protection of Information

The contractor shall be responsible for properly protecting all information used, gathered, or developed as a result of work under this contract. The contractor shall also protect all Government data, equipment, etc. by treating the information in accordance with its FISMA system categorization.

All information about the systems gathered or created under this contract should be considered as CUI information. If contractor personnel must remove any information from the primary work area that is included in the ATO boundary, they should protect it to the same FedRAMP requirements. The use of any information that is subject to the Privacy Act will be utilized in full accordance with all rules of conduct as applicable to Privacy Act Information.

5.7.1 Unrestricted Rights to Data

The government will retain unrestricted rights to government data. The ordering activity retains ownership of any user created/loaded data and applications hosted on vendor's infrastructure, as well as maintains the right to request full copies of these at any time.

5.7.2 Personally Identifiable Information

Personally identifiable information (PII) **<SELECT: is or is not>** in the scope of acquisition and PII **<SELECT: is or is not>** expected to be stored in the vendor's cloud solution. The vendor shall prepare a Privacy Threshold Assessment (PTA) to either document PII is not in scope, or determine which categories of information will be stored, processed, or transmitted by the system. The use of any information that is subject to the Privacy Act will be utilized in full accordance with all rules of conduct as applicable to Privacy Act Information.

PII (should it come into scope) will require the following guidelines be adhered to.

- The vendor's information system must be authorized at least at the FIPS PUB 199 Moderate level.
- For any system that collects, maintains or disseminates PII, a PIA must be completed by the contractor and provided to the GSA Privacy Office for review along with the other authorization to operate (ATO) documents.
- If the system retrieves information using PII, the Privacy Act applies and it must have a system of records notice (SORN) published in the Federal Register.
- If PII is collected from individuals by the system, a Privacy Act Statement (i.e., Privacy Notice) must be provided to users prior to their use of the application on what data is being collected and why, as well as the authority for the collection and the impact of not providing some or all of it. The Privacy Act Statement must be available to the individual directly on the form used to collect the information. Providing a link back to the Statement from the form is acceptable.

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

5.7.3 Data Availability

The data must be available to the Government upon request within one business day or within the timeframe negotiated with the Contractor, and shall not be used for any other purpose other than that specified herein. The contractor shall provide requested data at no additional cost to the government.

5.7.4 Data Release

Any information made available to the Contractor by the Government shall be used only for the purpose of carrying out the provisions of this contract and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of the contract. In performance of this contract, the Contractor assumes responsibility for protection of the confidentiality of Government records and shall ensure that all work performed by its subcontractors shall be under the supervision of the Contractor or the Contractor's responsible employees. Each officer or employee of the Contractor or any of its subcontractors to whom any Government record may be made available or disclosed shall be notified in writing by the Contractor that information disclosed to such officer or employee can be used only for that purpose and to the extent authorized herein. Further disclosure of any such information, by any means, for a purpose or to an extent unauthorized herein, may subject the offender to criminal sanctions imposed by 18 U.S.C. §§ 1030.

Contractor will not disclose Customer Data to any government or third party or access or use Customer Data; except in each case as necessary to maintain the Cloud Services or to provide the Cloud Services to Customer in accordance with this contract, or as necessary to comply with the law or a valid and binding order of a governmental or regulatory body (such as a subpoena or court order). Unless it would be in violation of a court order or other legal requirement, the Contractor will give the Government reasonable notice of any such legal requirement or order, to allow the Government to seek a protective order or other appropriate remedy.

5.8 Data Ownership

All Government data collected in the system is the property of the Federal Government. All data collected by the system shall be provided by the Contractor (system provider) as requested during the contract period and at the completion of the contract period.

5.9 Confidentiality and Nondisclosure

Personnel working on any of the described tasks, may at Government request, be required to sign formal non-disclosure and/or conflict of interest agreements to guarantee the protection and integrity of Government information and documents.

Additionally, any information made available to the Contractor by the Government shall be used only for the purpose of carrying out the provisions of this contract and shall not be divulged or made known in any manner to any persons except as may be necessary in the

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

performance of the contract. In performance of this contract, the Contractor assumes responsibility for protection of the confidentiality of Government records and shall ensure that all work performed by its subcontractors shall be under the supervision of the Contractor or the Contractor's responsible employees. Each officer or employee of the Contractor or any of its subcontractors to whom any Government record may be made available or disclosed shall be notified in writing by the Contractor that information disclosed to such officer or employee can be used only for that purpose and to the extent authorized herein. Further disclosure of any such information, by any means, for a purpose or to an extent unauthorized herein, may subject the offender to criminal sanctions imposed by 18 U.S.C. §§ 1030.

5.10 GSA Non-Disclosure Agreement

Each individual contractor/subcontractor employee who performs work on this contract is required to sign an Employee NDA. The Contractor shall submit to the COR a completed confidentiality and NDA for each individual contractor/subcontractor.

The Contractor and all contractor/subcontractor employees may have access to sensitive data, proprietary, or confidential business information of other companies or the Government in the course of performing official duties on this contract. The term "proprietary information" means any information considered so valuable by its owners that it is held in secret by them and their licensees and is not available to the public.

All information that is (1) obtained related to or derived from this contract, and (2) results from or derived from any actual tasks assigned to contractor employees while participating on this contract is considered proprietary.

The Contractor and all contractor/subcontractor employees will not use vendor proprietary information except as necessary to perform this contract, and shall agree not to disclose such information to third parties, including any employee of the contractor/subcontractor who has not executed this NDA, or use such information in any manner inconsistent with the purpose for which it was obtained. Anyone failing to comply with the agreement may be subject to disciplinary action or termination of employment by the contractor/subcontractor, and possible administrative, civil, or criminal penalties.

Note: GSA's Office of the General Counsel (OGC) is available to coordinate on defining NDA requirements. Upon request, GSA OGC can advise on NDA development.

5.11 Additional Stipulations

1. When containing sensitive information, deliverables shall be labeled Controlled Unclassified Information (CUI) or contractor selected designation per document sensitivity. Not all deliverables contain CUI. When in question, the contractor should use the National Archives and Records Administration (NARA) CUI Registry to help determine the appropriate designation for marking. External transmission/dissemination of CUI to or from a Government computer must be

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

encrypted. Certified encryption modules must be used in accordance with FIPS PUB 140-2[7], *"Security Requirements for Cryptographic Modules."*

2. The Contractor shall certify applications are fully functional and operate correctly as intended on systems using benchmarks from GSA technical guidelines, NIST guidelines, Center for Internet Security guidelines, or industry best practice guidelines, as reviewed and accepted by the GSA AO. The standard installation, operation, maintenance, update, and/or patching of software shall not alter the configuration settings from the approved benchmark configuration. Information technology for Windows systems should use the Windows Installer Service for installation to the default "program files" directory and should be able to silently install and uninstall. Applications designed for normal end users shall run in the standard user context without elevated system administration privileges. The contractor shall use tools to verify their products operate correctly with the approved benchmark configurations and do not alter the benchmark settings.

3. The contractor shall cooperate in good faith in defining NDA that other third parties must sign when acting as the Federal government's agent.

Note: GSA's Office of the General Counsel (OGC) is available to coordinate on defining NDA requirements. Upon request, GSA OGC can advise on NDA development.

4. The contractor shall comply with any additional FedRAMP privacy requirements.
5. The Government has the right to perform manual or automated audits, scans, reviews, or other inspections of the vendor's IT environment being used to provide or facilitate services for the Government. The Contractor shall be responsible for the following privacy and security safeguards:
    a. The Contractor shall not publish or disclose in any manner, without the Contracting Officer's written consent, the details of any safeguards either designed or developed by the Contractor under this contract or otherwise provided by the Government. Exception - Disclosure to a Consumer Agency for purposes of A&A verification or to the MAX.Gov portal. To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data, the Contractor shall afford the Government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases within 72 hours of the request. Access to support incident investigations, shall be provided as soon as possible but not longer than 72 hours after request.
    b. Physical Access Considerations – If the SaaS provider is operated within an IaaS that is FedRAMP authorized (e.g., AWS); physical access to the physical datacenter environment will be governed by the terms of access allowed by the

[7] NIST has issued FIPS 140-3, FIPS 140-2 modules are still being validated and will be accepted through September 22, 2026. For additional information see the NIST cryptographic module validation program webpage.

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

underlying infrastructure provider as defined in the FedRAMP A&A authorization package.

c. The program of inspection shall include, but is not limited to:

- Authenticated and unauthenticated operating system/network vulnerability scans
- Authenticated and unauthenticated web application vulnerability scans
- Automated scans can be performed by Government personnel, or agents acting on behalf of the Government, using Government operated equipment, and Government specified tools. If the vendor chooses to run its own automated scans or audits, results from these scans may at the Government's discretion, be accepted in lieu of Government performed vulnerability scans. In these cases, scanning tools and their configuration shall be approved by the Government. In addition, the results of vendor-conducted scans shall be provided in full to the Government.

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

6. The Contractor shall comply with Section 1634 of Public Law 115-91 that prohibits use of any hardware, software, or services developed or provided, in whole or in part, by— (1) Kaspersky Lab (or any successor entity); (2) any entity that controls, is controlled by, or is under common control with Kaspersky Lab; or (3) any entity of which Kaspersky Lab has majority ownership.

7. The Contractor shall comply with 52.204-25 of the Federal Acquisition Regulation (FAR). It prohibits, under Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232), contractors from providing to the Government any equipment, system, or service that uses telecommunications equipment or video surveillance services from certain named companies as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception or waiver is granted per the FAR. It also prohibits, under Section 889(a)(1)(B), contractors from using any equipment, system, or service that uses telecommunications or video surveillance equipment or services from certain named companies as a substantial or essential component of any system or as critical technology as part of any system, unless an exception or waiver is granted per the FAR. The proscribed companies are Huawei Technologies Company, ZTE Corporation, Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, and Dahua Technology Company and their subsidiaries and affiliates.

5.12 References

CSP Authorization Playbook-Getting Started with FedRAMP

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

6 Mobile Application - IT Security and Privacy Requirements

The contractor shall generally, substantially, and in good faith follow GSA IT Security Policy and Guidelines including GSA Order CIO 2100.1, "*GSA Information Technology (IT) Security Policy"* and GSA IT Security Procedural Guide 12-67, "*Securing Mobile Devices and Applications,*" or current versions. In situations where there are no procedural guides, the contractor shall use generally accepted industry best practices for IT security.

6.1 General Mobile Application Guidelines

1. The Mobile Application (App) shall be integrated with a Mobile Device Management (MDM) solution. GSA currently uses MAAS 360.
2. The contractor shall provide to the GSA IT Contracting Officer Representative (COR) the source code and all supporting artifacts of the app for security testing via the GSA Static and mobile Code Scanning program. In addition, the contractor shall actively participate in the program to remediate all findings according to the most recent Static Code Scanning Standard Operating Procedure (SOP) before the beta and production App is accepted by GSA. Once the contract is awarded, GSA will provide a copy of the Static Code Scanning SOP to the contractor.
3. The contractor shall provide clear and concise documentation so that future developers and programmers can understand the processes used and are able to enhance, edit or build upon the original App. All source code information prepared for this App is the property of GSA, Federal Acquisition Service, OCCM and GSA IT.
    - The contractor shall provide detailed process and code documentation.
    - The contractor shall provide App features documentation.
    - The contractor shall support development and updates of a security authorization package for the App following the process requirements documented in GSA IT Security Procedural Guide 12-67, "*Securing Mobile Devices and Applications,"* or current version.

6.2 Mobile Device Security

The contractor shall adhere to the following requirements and guidelines for developing mobile applications. All requirements and guidelines are found in the GSA IT Security Procedural Guide 12-67, "*Securing Mobile Devices and Applications,"* which will be provided upon contract award.

A mobile application, most commonly referred to as an app, is a type of application software designed to run on a mobile device, such as a smartphone or tablet computer. Mobile applications frequently serve to provide users with similar services to those accessed on PCs. Apps are generally small, individual software units with limited capabilities and isolated functionality. The simplest apps are developed to utilize the web browser of the mobile device to provide a feature set integration much like what is found on a user's PC. However, as mobile

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

app development has grown, a more sophisticated approach involves developing applications specifically for the mobile environment, taking advantage of both its limitations and advantages. For example, apps that use location-based features are inherently built from the ground up with an eye to mobile devices given that you do not have the same concept of location on a PC. With this new paradigm in both mobile platforms and the applications loaded on them, GSA will concentrate security focus on the following goals:

- That all apps loaded have an initial assessment by GSA for acceptability and then a security assessment & authorization, when required
- That all apps are deployed from only trusted sources, following their security/assessment process – This presently is the Apple ITunes store for iOS and the Google Play store for Android. MaaS360 may also be used, once retrieved from these sources, for enterprise deployment
- That Terms of Service (ToS) discipline is adhered to, based on acceptability of an app – either as an individual user or for GSA as an Agency
- That apps deemed to be unacceptable are blacklisted, using MaaS360
- That a mobile app inventory for all devices be maintained
- That GSA developed apps are assessed, evaluated and approved by the AO for the system they support before deployment

6.3 Application Sources

Allowing mobile apps to be loaded from an unknown source presents one of the greatest risks to GSA's environment when using mobile devices. "Side loading" of apps is a process where a user installs an application from a source other than the Apple ITunes store or Google Play store. If a user jailbreaks a device, side loading can occur as well. Jailbreaking, or rooting, is a process where an Operating System (OS) of a mobile device grants a user or application root level access to the OS. While iOS devices that are not jailbroken/rooted protect against sideloading, the Android OS allows a user to turn such protection on/off (allow unknown sources) if not managed by MDM.

As such, the following policies apply to all GSA devices (Government and Bring Your Own Device) used in the environment to protect against side loading of apps:

- Devices shall not be jailbroken/rooted by users or apps loaded by users. GSA's MDM solution shall immediately notify an administrator of all such incidents immediately for remediation.
- Unknown sources shall not be enabled by users or applications. GSA's MDM solution shall immediately notify an administrator of all such incidents for remediation.
- GSA developed apps may be sideloaded for testing purposes only on test devices, but production deployment of GSA developed apps may only be done via the policies outlined below for Apple iOS and Google Android.

The GSA MaaS store may be employed for enterprise deployments, but only after the app has undergone the review/approval processes outlined below:

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

- Apple App Review guidelines
- Google Play Store Developer Policy Center

6.4 Terms of Service (ToS)

Many terms found in commercial TOS or End User License Agreements (EULA) are not acceptable when the Government is the end user. The Office of Chief Information Officer (OCIO) requires that software and services within the GSA Enterprise have approved ToS or EULA.

Apps deemed to be acceptable are loaded at the discretion of the user for either personal use or as a personal productivity tool to further enhance the work experience. As such, use of the App is not mandated by the agency. Therefore, acceptance of the ToS falls upon the user as an individual. This is true even if the App is loaded using a GSA.gov domain account or registered with a user's GSA.gov email address.

Apps that are approved after formal assessment: and include a formal review by GSA Counsel as part of the review/approval process, where the ToS was found to be acceptable to the government or a modified ToS was negotiated as part of the approval review, prior to final authorization. When loaded and activated, the user is accepting the ToS (often a technical function required of the user), not as an individual, but as an employee or contract employee assigned to perform work functions for GSA.

6.5 GSA Privacy Requirements

Personally identifiable information (PII) **<SELECT: is or is not>** in the scope of the acquisition and PII **<SELECT: is or is not>** expected to be stored, processed, or transmitted in the vendor's App. The collection, maintenance or dissemination of any PII that is subject to the Privacy Act and/or the E-Government Act will be handled in full accordance with all GSA rules of conduct and in accordance with GSA Privacy Program requirements.

The contractor shall work with GSA to prepare a Privacy Threshold Assessment (PTA) to confirm and document PII is not in scope, or to determine which categories of information will be stored, processed, or transmitted by the App. The PTA must be completed before development begins and whenever a change with privacy impact (e.g., a new category of information is collected) is made to an existing App. PTAs are required to determine whether a Privacy Impact Assessment (PIA) and/or a System of Records Notice (SORN) is required, and if any other privacy requirements apply to the App. Information regarding PIAs can be found in this GSA Policy.

PII (should it come into scope) will require the following guidelines be adhered to.

- The vendor's App must be authorized at least at the FIPS PUB 199 Moderate level.
- For any system that collects, maintains or disseminates PII, a PIA must be completed by the contractor and provided to the GSA Privacy Office for review along with the other authorization to operate (ATO) documents.

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

- If the system retrieves information using PII, the Privacy Act applies and it must have a system of records notice (SORN) published in the Federal Register.
- If PII is collected from individuals by the system, a Privacy Act Statement (i.e., Privacy Notice) must be provided to users prior to their use of the application on what data is being collected and why, as well as the authority for the collection and the impact of not providing some or all of it. The Privacy Act Statement must be available to the individual directly on the form used to collect the information. Providing a link back to the Statement from the form is acceptable.

Per OMB A-130 Privacy Act Statements must include:

(1) the authority (whether granted by statute or executive order) that authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary;
(2) the principal purpose(s) for which the information is intended to be used;
(3) the published routine uses to which the information is subject;
(4) the effects on the individual, if any, of not providing all or any part of the requested information; and
(5) an appropriate citation (and, if practicable, a link) to the relevant SORN(s).

An example Privacy Act Statement is available at GSA's Privacy Act Statement for Design Research webpage.

Note: Apps that access data a user creates must assume a user may include privacy data/PII in the application unless the data creation is restricted to data controlled by the App.

All contractor staff who have significant privacy information responsibilities must complete GSA's mandatory privacy awareness and role-based training courses. This includes contractors who work with PII as part of their work duties (e.g., Human Resource staff, Finance staff, and managers/supervisors).

6.6 GSA App Development, Assessment, Authorization and Deployment

GSA developed apps are designed to take advantage of the concept of Anytime, Any Where, Any Device (A3) to allow GSA users and customers to access GSA data while mobile. As such, as GSA business lines develop apps for use on the iOS and Android environment, these apps must undergo an assessment and authorization process before being deployed. With that in mind, the following guidelines are to be followed:

- A GSA developed app that supports a GSA FISMA system must be documented in the System Security and Privacy Plan and authorized to operate as part of a current ATO letter from the respective AO before deployment. GSA IT Security Procedural Guide 06-30, *"Managing Enterprise Cybersecurity Risk,"* is to be followed for this process. Any app that is not directly tied to an already existing system authorized to operate must have

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

an assessment performed and subsequently approved for release by the Chief Information Security Officer (CISO).

- Any mobile app development shall result in a minimum of the release of both an iOS and Android version of the app. This ensures coverage to all users within GSA and the maximum coverage for apps released to the public. Any additional application versions for alternate OS mobile platforms may be developed for such apps, but iOS and Android shall remain as the core base OS' for GSA developed mobile apps for all releases.
- All GSA developed apps must follow the respective application review and publication guidelines for the OS to which they were developed as outlined in Section 8.2 of GSA IT Security Procedural Guide 12-67, "*Securing Mobile Devices and Applications"* and the release process documented in this section.
- Other than for testing purposes on non-user provisioned mobile devices, side loading of apps in the environment is not authorized.
- The GSA MaaS360 Store is authorized for enterprise deployment of apps to GSA user devices once that app has been assessed, authorized, and published according to the guidelines outlined in this section.
- Mobile code scanning throughout the development cycle is critical, but before release by the Mobile Device Team, a mobile app must be scanned by the Systems Engineering Division (ISE) Team within the OCISO. This scan is a source code scan using the CheckMarx platform. As with all applications in GSA, no High/Critical findings are allowed from these scan results. Moderate findings should be documented in the respective POA&M for the system by which the app is authorized and accepted by the AO; Low and Informational findings should be taken into consideration by the developers for their next iteration of app development. A detailed process for mobile app release is documented at the end of this section.
- All mobile application development should take into consideration the Open Web Application Security Project (OWASP) Mobile Security Project when developing mobile apps either within GSA or for use by the general public. The guidelines for mobile application security testing from OWASP are linked below:
  - OWASP Mobile Security Testing Guide
  - OWASP Mobile Security Project Home Page
- GSA developed mobile apps must undergo an assessment review and approval process before being released for use. These apps fall into two categories that shall have slightly different processes for approval, with many common steps.
- Mobile apps that are developed as part of another system with a current ATO and provide access to an application using a different form factor (smartphones/tablets), such apps must be documented in the System Security and Privacy Plan for the system they support.

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

- Mobile apps designed for a specific purpose not part of a current ATO stand alone in their ATO. As these apps do not have a parent system they support, the below listed process is the complete assessment process required for these apps.

All apps must follow the approval processes outlined below:

1. Apps must be scanned prior to release by the GSA Office of the CISO using the Checkmarx Application scanner. No Critical/High findings may remain for approval to be received and any moderate/medium findings must be contained in a POA&M, either for the system the app is a part of, or a separate POA&M if a standalone mobile app.
2. The privacy requirements as stated above must be met.
3. A mobile application security assessment review in accordance with the GSA-IT Procedural Guide: CIO-IT Security-12-67, "*Securing Mobile Devices and Applications*" must be completed and signed by the mobile App owner, mobile App assessor, mobile App Information System Security Manager (ISSM), a representative of the Office of the CSIO, to denote a proper assessment and review was conducted of the mobile app prior to release.

6.7 Intellectual Property

This task order is funded by the United States Government. All intellectual property generated and/or delivered pursuant to this Firm-Fixed Price Statement of Work will be subject to appropriate federal acquisition regulations which entitle the Government to unlimited license rights in technical data and computer software developed exclusively with Government funds, a nonexclusive "paid-up" license to practice any patentable invention or discovery made during the performance of this task order, and a "paid-up" nonexclusive and irrevocable worldwide license to reproduce all works (including technical and scientific articles) produced during this task order.

6.8 Confidentiality and Nondisclosure

The preliminary and final deliverables and all associated working papers and other material deemed relevant by the agency that have been generated by the contractor in the performance of this contract, are the property of the U.S. Government and must be submitted to the COR at the conclusion of the contract. The U.S. Government has unlimited data rights to all deliverables and associated working papers and materials.

All documents produced for this project are the property of the U.S. Government and cannot be reproduced or retained by the contractor. All appropriate project documentation will be given to the agency during and at the end of this contract. The contractor shall not release any information without the written consent of the Contracting Officer.

Personnel working on any of the described tasks may, at Government request, be required to sign formal non-disclosure and/or conflict of interest agreements (NDA/COI) to guarantee the protection and integrity of Government information and documents.

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

Additionally, any information made available to the Contractor by the Government shall be used only for the purpose of carrying out the provisions of this contract and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of the contract. In performance of this contract, the Contractor assumes responsibility for protection of the confidentiality of Government records and shall ensure that all work performed by its subcontractors shall be under the supervision of the Contractor or the Contractor's responsible employees. Each officer or employee of the Contractor or any of its subcontractors to whom any Government record may be made available or disclosed shall be notified in writing by the Contractor that information disclosed to such officer or employee can be used only for that purpose and to the extent authorized herein. Further disclosure of any such information, by any means, for a purpose or to an extent unauthorized herein, may subject the offender to criminal sanctions imposed by 18 U.S.C. §§ 1030.

6.9 GSA Non-Disclosure Agreement

Each individual contractor/subcontractor employee who performs work on this contract is required to sign an Employee NDA. The Contractor shall submit to the COR a completed confidentiality and NDA form for each individual contractor/subcontractor.

The Contractor and all contractor/subcontractor employees may have access to sensitive data, proprietary, or confidential business information of other companies or the Government in the course of performing official duties on this contract. The term "proprietary information" means any information considered so valuable by its owners that it is held in secret by them and their licensees and is not available to the public.

All information that is (1) obtained related to or derived from this contract, and (2) results from or derived from any actual tasks assigned to contractor employees while participating on this contract is considered proprietary.

The Contractor and all contractor/subcontractor employees will not use vendor proprietary information except as necessary to perform this contract, and shall agree not to disclose such information to third parties, including any employee of the contractor/subcontractor who has not executed this NDA, or use such information in any manner inconsistent with the purpose for which it was obtained. Anyone failing to comply with the agreement may be subject to disciplinary action or termination of employment by the contractor/subcontractor, and possible administrative, civil, or criminal penalties.

Note: GSA's Office of the General Counsel (OFC) is available to coordinate on defining NDA requirements. Upon request, GSA OGC can advise on NDA development.

6.10 Personnel Security Requirements

Contractor shall furnish documentation reflecting favorable adjudication of background investigations for all personnel (including subcontractors) supporting the system. Contractors shall comply with GSA Order 2100.1, "*GSA Information Technology (IT) Security Policy"* and GSA

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

Order ADM 2181.1, "*Homeland Security Presidential Directive-12, Personal Identity Verification and Credentialing, and Background Investigations for Contractors."* GSA separates the risk levels for personnel working on Federal computer systems as follows:

- A favorable initial fitness/suitability determination must be granted and a Tier 1 or higher background investigation initiated before access to the GSA network or any GSA IT system. There shall be no waivers to this requirement for GSA network and IT system access for GSA employees or contractors.
- A favorable initial fitness/suitability determination must be granted and a Tier 2 or higher background investigation initiated before access to PII/CUI is granted. The authority and access shall be determined by the appropriate GSA Supervisor (for GSA employees) or CO (for contract personnel), Data Owner, and the System's AO. Each System's AO, with the request of the GSA Supervisor, Data Owner or CO, shall evaluate the risks associated with each such request.
- A favorable suitability determination must be completed at a Tier 2 or higher background investigation before privileged access to the GSA network or IT systems is granted. A waiver may be requested in order to maintain GSA business operations; however such requests should be used judiciously and not incur unnecessary risks to GSA.

If final adjudication of a background investigation is unfavorable, GSA network and IT system access must be revoked, and any GFE, including the GSA PIV card, must be retrieved and returned to OMA.

GSA shall sponsor the investigation when deemed necessary. No access shall be given to government computer information systems and government sensitive information without a background investigation being verified or in process. If results of background investigation are not acceptable, then access shall be terminated.

The Contractor shall provide a report of separated staff on a monthly basis, beginning 60 days after execution of the option period.

6.11 Additional Stipulations

1. When containing sensitive information, deliverables shall be labeled Controlled Unclassified Information (CUI) or contractor selected designation per document sensitivity. Not all deliverables contain CUI. When in question, the contractor should use the National Archives and Records Administration (NARA) CUI Registry to help determine the appropriate designation for marking. External transmission/dissemination of CUI to or from a Government computer must be encrypted. Certified encryption modules must be used in accordance with FIPS PUB 140-2[8], "Security requirements for Cryptographic Modules."

[8] NIST has issued FIPS 140-3, FIPS 140-2 modules are still being validated and will be accepted through September 22, 2026. For additional information see the NIST cryptographic module validation program webpage.

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

2. The Contractor shall certify mobile applications are fully functional and operate correctly as intended on mobile devices in accordance with GSA IT Security Procedural Guide 12-67, "*Securing Mobile Devices and Applications*." The standard installation, operation, maintenance, update, and/or patching of mobile applications shall not alter configuration settings as documented in CIO-IT Security-12-67. Mobile applications designed for normal end users shall run in the standard user context without elevated administration privileges.
3. The Contractor shall cooperate in good faith in defining NDAs that other third parties must sign when acting as the Federal government's agent.

Note: GSA's Office of the General Counsel (OGC) is available to coordinate on defining NDA requirements. Upon request, GSA OGC can advise on NDA development.

4. The Government has the right to perform manual or automated audits, scans, reviews, or other inspections of the vendor's IT environment being used to provide or facilitate services for the Government. The Contractor shall be responsible for the following privacy and security safeguards:
    a. The Contractor shall not publish or disclose in any manner, without the Contracting Officer's written consent, the details of any safeguards either designed or developed by the Contractor under this contract or otherwise provided by the Government. Exception - Disclosure to a Consumer Agency for purposes of A&A verification or to the MAX.Gov portal. To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data, the Contractor shall afford the Government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases within 72 hours of the request. Access to support incident investigations, shall be provided as soon as possible but not longer than 72 hours after request.

        The program of inspection shall include, but is not limited to:

        - Authenticated and unauthenticated operating system/network vulnerability scans
        - Authenticated and unauthenticated web application vulnerability scans
        - Authenticated and unauthenticated database application vulnerability scans
        - Automated scans can be performed by Government personnel, or agents acting on behalf of the Government, using Government operated equipment, and Government specified tools. If the vendor chooses to run its own automated scans or audits, results from these scans may at the Government's discretion, be accepted in lieu of Government performed vulnerability scans. In these cases, scanning tools and their configuration shall be approved by the Government. In addition, the results of vendor-conducted scans shall be provided in full to the Government.

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

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

5. The Contractor shall comply with Section 1634 of Public Law 115-91 that prohibits use of any hardware, software, or services developed or provided, in whole or in part, by— (1) Kaspersky Lab (or any successor entity); (2) any entity that controls, is controlled by, or is under common control with Kaspersky Lab; or (3) any entity of which Kaspersky Lab has majority ownership.

6. The Contractor shall comply with 52.204-25 of the Federal Acquisition Regulation (FAR). It prohibits, under Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232), contractors from providing to the Government any equipment, system, or service that uses telecommunications equipment or video surveillance services from certain named companies as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception or waiver is granted per the FAR. It also prohibits, under Section 889(a)(1)(B), contractors from using any equipment, system, or service that uses telecommunications or video surveillance equipment or services from certain named companies as a substantial or essential component of any system or as critical technology as part of any system, unless an exception or waiver is granted per the FAR. The proscribed companies are Huawei Technologies Company, ZTE Corporation, Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, and Dahua Technology Company and their subsidiaries and affiliates.

7 Nonfederal Systems and Organizations – IT Security and Privacy Requirements

7.1 Required Policies and Regulations for GSA Contracts

Federal Laws, Regulations, and Guidance:

The contractor shall comply with all applicable Federal Laws, Regulations, and Guidance.

- FISMA of 2014, "*The Federal Information Security Modernization Act of 2014*"
- Privacy Act of 1974, "*5 USC, § 552a*"
- E-Government Act of 2002 section 208, "*44 USC 3501*"
- 32 CFR Part 2002, "*Controlled Unclassified Information*"
- OMB Circular A-108, "*Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*"
- OMB Memo 03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002"

Federal Standards and Guidance:

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

The contractor shall comply with the following Federal Information Processing Standards (FIPS) and NIST guidelines.

- FIPS PUB 200, "*Minimum Security Requirements for Federal Information and Information Systems*"
- NIST SP 800-53, Revision 5, "*Security and Privacy Controls for Information Systems and Organizations*"
- NIST SP 800-171, Revision 2, "*Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*"
- NIST SP 800-171A, "*Assessing Security Requirements for Controlled Unclassified Information*"

GSA Policies:

The contractor shall comply with the following GSA Directives/Policies.

- GSA Order CIO 1878.3, "*Developing and Maintaining Privacy Threshold Assessments, Privacy Impact Assessments, Privacy Act Notices, and System of Records Notices*"
- GSA Order CIO 2100.1, "*GSA Information Technology (IT) Security Policy*"
- GSA Order CIO 2103.1, "*Controlled Unclassified Information (CUI) Policy*"
- GSA Order CIO 2200.1, "*GSA Privacy Act Program*"
- GSA Order CIO 9297.2, "*GSA Information Breach Notification Policy*"

GSA Procedural Guides:

- GSA IT Procedural Security Guides 01-02, *"Incident Response"*
- GSA CIO IT Security Procedural Guide 09-44, "*Plan of Action and Milestones (POA&M)"*
- GSA IT Security Procedural Guide 11-51, *"Conducting Penetration Test Exercises*"

Note: GSA's Procedural Guides are updated frequently; to make sure you have the most recent version of publicly available procedural guides, visit GSA.gov. If a non-publicly available guide is needed, contact the contracting officer who will coordinate with the GSA Office of the Chief Information Security Officer to determine if it can be made available.

7.2 GSA Security Compliance Requirements

To comply with the Federal standard, nonfederal systems and organizations shall implement the specific security requirements in NIST SP 800-171, Revision 2, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations" for protecting the confidentiality of Controlled Unclassified Information (CUI). NIST SP 800-171 controls requirements have been tailored for non-federal entities, eliminating requirements, controls, or parts of controls that are uniquely Federal, not directly related to protecting the confidentiality of CUI; or expected to be routinely satisfied by nonfederal organizations without specification. NIST SP 800-171 controls are derived from FIPS PUB 200, "Minimum Security Requirements for Federal Information and Information Systems," and the moderate security control baseline in NIST SP 800-53, Revision 5, "Security and Privacy Controls for Information Systems and

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

Organizations," and are based on the CUI regulation 32 CFR Part 2002, "Controlled Unclassified Information."

The basic and derived security requirements in NIST SP 800-171 provide protection from unauthorized disclosure and unauthorized modification of CUI. The requirements apply only to the components of non-federal systems that process, store, or transmit CUI, or that provide security protection for such components.

7.3 Security Assessment Activities and Required Documentation

The non-federal system/organization shall implement the NIST SP 800-171, Revision2 controls; conduct an independent security assessment using NIST SP 800-171A, "*Assessing Security Requirements for Controlled Unclassified Information*" with results documented in a security assessment report; and security vulnerabilities or gaps in security requirements documented in a Plan of Action and Milestones. The resultant documents including the System Security and Privacy Plan, Security Assessment Report, and Plan of Action and Milestones will be critical inputs to a risk management decision by the GSA to process, store, or transmit CUI on a system hosted by a nonfederal organization and whether it is advisable to pursue an agreement or contract with the non-federal organization. The failure to implement the NIST SP 800-171, Revision 2 controls and maintain the supporting documentation will result in the termination of the contract. The non-federal system must have a new independent security assessment conducted at least every three (3) years or at the discretion of the GSA when there is a significant change to the system's security posture or via continuous monitoring. Documents that contain CUI must be marked as such. Not all deliverables contain CUI. When in question, the contractor should use the NARA CUI Registry to help determine the appropriate designation for marking, handling or transmitting. The contractor shall create, maintain and update the following security documentation and make available to the Government:

- **System Security and Privacy Plan (SSPP)** completed in agreement with NIST SP 800-171, Revision 2, "*Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*" using the template provided by the GSA.
- **Security Assessment Report (SAR)** completed in accordance with NIST SP 800-171A, "*Assessing Security Requirements for Controlled Unclassified Information*" using the template provided by the GSA. Nonfederal information systems must have an independent assessment performed and authorized every three (3) years or whenever there is a significant change to the non-federal system's security posture. The independent assessor shall be a FedRAMP accredited Third Party Assessment Organizations (3PAOs) or be approved by the GSA if not a 3PAO.
- **Plan of Action & Milestones** (POA&M) document completed in accordance with GSA IT Security Procedural Guide 09-44, *"Plan of Action and Milestones (POA&M)*."
- **Penetration Test Report** (Not required; recommended only) documenting the results of an independent exercise. Reference GSA IT Security Procedural Guide 11-51, *"Conducting Penetration Test Exercises"* for penetration testing guidance.

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

7.4 Reporting and Continuous Monitoring

Maintenance of security will be through continuous monitoring of security controls of the non-federal system and its environment of operation to determine if the security controls in the information system continue to be effective over time in light of changes that occur in the system and environment. Through continuous monitoring, security controls and supporting deliverables are updated and submitted to GSA per the schedules below. The submitted deliverables (or lack thereof) provide a current understanding of the security state and risk posture of the information system(s). They allow GSA to make credible risk-based decisions regarding the continued usage of non-federal systems and initiate appropriate responses as needed when changes occur.

Deliverables to be provided Quarterly to the GSA Information System Security Officer (ISSO), Information System Security Manager (ISSM), and/or Contracting Officer (COR)

1. Vulnerability Scanning
   Reference: NIST SP 800-171, Revision 2 Security Requirement 3.11.2
   Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified. Provide the most recent Web Application and Operating System vulnerability scan reports.
2. Plan of Action & Milestones (POA&M) Update
   Reference: NIST SP 800-171, Revision 2 Security Requirement 3.12.2
   Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems. Provide POA&M updates in accordance with requirements and the schedule set forth in GSA CIO IT Security Procedural Guide 09-44, "*Plan of Action and Milestones (POA&M)*."

Deliverables to be provided Annually or when there is a major change to the GSA ISSO, ISSM, and/or COR

1. Updated System Security and Privacy Plan
   Reference: NIST 800-171, Revision 2 Security Requirement 3.12.4
   Develop, document, and periodically update system security and privacy plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems. The System Security and Privacy Plan must be in accordance with NIST SP 800-171, Revision 2, using the Security and Privacy Plan template provided by the GSA.

Deliverables to be provided every three years or when there is a major change to the GSA ISSO, ISSM, and/or COR

1. Security Assessment Report
   Reference: NIST 800-171, Revision 2 Security Requirement 3.12.1
   Periodically assess the security controls in organizational systems to determine if the controls are effective in their application. Deliver the results of the security assessment

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

conducted using the assessment procedures in NIST SP 800-171A, "*Assessing Security Requirements for Controlled Unclassified Information*", using the Security Assessment Report template provided by the GSA.

7.5 Privacy Assessment Activities and Required Documentation

Assessment of the privacy posture of the non-federal system and its environment of operation will be through continuous monitoring of privacy controls to determine if they remain effective over time in light of changes that occur in the system and environment. Through continuous monitoring, privacy controls and supporting deliverables are updated and submitted to GSA per the schedules below. The submitted deliverables (or lack thereof) provide a current understanding of the privacy risk posture of the information system(s). They allow GSA to make credible risk-based decisions regarding the continued protection of CUI residents in non-federal systems and initiation of appropriate responses as needed when changes occur.

Deliverables to be provided Annually or when there is a major change to the GSA ISSO, ISSM, and/or COR

1. Privacy Threshold Assessment (PTA)
   Reference: NIST SP 800-171 Revision 2 Security Requirement 3.1.9 and 3.1.22
   The contractor shall prepare a PTA to confirm and document whether Personally Identifiable Information (PII) is in scope or not, and to determine which other categories of CUI will be stored, processed, or transmitted by the system. The PTA must be completed before GSA begins using the non-federal system.

   If through the initial PTA GSA finds that no PII or other CUI is in scope, then vendor shall both:
   a. Recertify the PTA on an annual basis to confirm the absence of such sensitive information; AND
   b. Update the PTA any time there is a change that may impact the privacy posture of the system or its environment of operation (e.g., collection of a new information type (see OMB Circular A-108, paragraph 6(b) for additional examples of significant changes requiring a PTA update).

If PII is in scope, deliverables to be provided every three years or when there is a major change to the GSA ISSO, ISSM, and/or COR

1. Privacy Impact Assessment (PIA)
   Reference: NIST SP 800-171 Revision 2 Security Requirement 3.12.1[9]
   For any system that collects, maintains or disseminates PII or other CUI, a PIA must be completed by the contractor and provided to the GSA Privacy Office for review. Then vendor shall:

[9] NIST SP 800-53 provides guidance on security and privacy controls for systems and organizations.

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

a. Limit system access to those with a Lawful Government Purpose; display login notifications or warning banners that CUI is present in the system and must be protected consistent with the CUI Program;
b. Prohibit any CUI from being posted or processed on publicly accessible systems;
c. Recertify the PIA every three years to confirm the collection, maintenance or dissemination of such sensitive information;
d. Update the PIA any time there is a change that may impact the privacy posture of the system or its environment of operation (e.g., collection of a new information type (see OMB Circular A-108, paragraph 6(b) for additional examples of significant changes requiring a PIA update).

OMB's PIA guidance: OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002
GSA's PIA guidance: GSA Privacy Impact Assessment Guidance for Nonfederal Systems

- If PII is in scope, the vendor shall include the following NIST SP 800-53, Revision 5 controls in its SSPP. Privacy controls are the administrative, technical, and physical safeguards employed within organizations to protect and ensure the proper handling of PII.

  AT-2: Literacy Training and Awareness
  AT-3: Role-based Training
  PL-4: Rules of Behavior
  PM-20: Dissemination of Privacy Program Information
  PM-22: Personally Identifiable Information Quality Management
  PM-25: Minimization of Personally Identifiable Information used in Testing, Training, and Research
  PM-26: Complaint Management
  PT-2: Authority to Process Personally Identifiable Information
  PT-3: Personally Identifiable Information Processing Purposes
  PT-4: Consent
  PT-5: Privacy Notice
  RA-8: Privacy Impact Assessment
  SA-4: Acquisition Process
  SA-8(33): Security and Privacy Engineering Principles | Minimization
  SA-9: External System Services
  SI-12(1): Information Management and Retention | Limit Personally Identifiable Information Elements

- A Privacy Policy/Notice shall be provided to users prior to their use of the application on what data is being collected and why, as well as the impact of not providing some or all of it. The Privacy Policy/Notice must be available to the individual directly on the form used to collect the information. Providing a link back to the Policy/Notice from the form is acceptable.

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

Other requirements: Government-approved terms of service.

7.6 Additional Stipulations

1. The Contractor shall comply with Section 1634 of Public Law 115-91 that prohibits use of any hardware, software, or services developed or provided, in whole or in part, by— (1) Kaspersky Lab (or any successor entity); (2) any entity that controls, is controlled by, or is under common control with Kaspersky Lab; or (3) any entity of which Kaspersky Lab has majority ownership.
2. The Contractor shall comply with 52.204-25 of the Federal Acquisition Regulation (FAR). It prohibits, under Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232), contractors from providing to the Government any equipment, system, or service that uses telecommunications equipment or video surveillance services from certain named companies as a substantial or essential component of any system, or as critical technology as part of any system , unless an exception or waiver is granted per the FAR. It also prohibits, under Section 889(a)(1)(B), contractors from using any equipment, system, or service that uses telecommunications or video surveillance equipment or services from certain named companies as a substantial or essential component of any system or as critical technology as part of any system, unless an exception or waiver is granted per the FAR. The proscribed companies are Huawei Technologies Company, ZTE Corporation, Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, and Dahua Technology Company and their subsidiaries and affiliates.

DocuSign Envelope ID: 9D69A644-AC81-4C2A-B568-05BB47791AE3

Appendix A: GSA Tailoring of NIST 800-53 Controls

The GSA Control Tailoring Workbook contains GSA defined values for NIST SP 800-53 Security and Privacy Controls. The workbook is not publicly available; contact the contracting officer who will coordinate with the GSA Office of the Chief Information Security Officer to determine if it can be made available.

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

IT Security Procedural Guide: Managing Enterprise Cybersecurity Risk
CIO-IT Security-06-30

Revision 23

May 9, 2022

Office of the Chief Information Security Officer

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

VERSION HISTORY/CHANGE RECORD

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
		Revision 1 – March 22, 2006		
1	Bo Berlas	Included the OWASP Web Application Penetration Checklist and the OWASP Testing Project documents as embedded objects into Appendix C – GSA Risk Assessment Security Requirements.	To provide a usable checklist for testing the OWASP Top Ten Vulnerabilities.	14
		Revision 2 – February 13, 2007		
1	Bo Berlas	Various updates to reflect changes in A&A process	FINAL publishing of NIST 800-53 on 12/2006	4-10
2	Bo Berlas	Updated Appendix A: Risk Assessment Report Format	RA and SA are now combined into a single RA/SA report.	11
3	Bo Berlas	Updated Appendix B: GSA Security Assessment Test Procedures	Updated Assessment test procedures based on FINAL publishing of NIST 800-53 on 12/2006	15
4	Bo Berlas	Updated Appendix C: Plan of Action and Milestone (POA&M) Template	Attached new POA&M template for FY 2007.	16
5	Bo Berlas	Updated Appendix D: Risk Assessment / Security Assessment Plan Template	Updated assessment plan template to reflect combining of RA and SA reports.	17
		Revision 3 – March 20, 2007		
1	Bo Berlas	Changed reference to OWASP Top Ten from 2007 Release Candidate 1 back to the 2004 Update.	OWASP Top Ten, 2007 RC1 has not been finalized. GSA will adopt the OWASP Top Ten, 2007 Update upon final publication.	6
2	Bo Berlas	New database scanning requirement.	App Detective or similar tool should be used to test database security configurations.	7
		Revision 4 – October 16, 2007		
1	Bo Berlas	Updated policy reference.	GSA IT Security Policy was updated June 2007.	6
2	Bo Berlas	Changed reference to OWASP Top Ten from the 2004 Update to the current 2007 Update.	The 2007 Top Ten lists current web application vulnerabilities.	7
3	Bo Berlas	Replaced the FY 2007 POA&M Reporting Template with the FY 2008 template.	New OMB Quarterly POA&M Reporting Requirements	17
		Revision 5 – July 15, 2010		
1	Bo Berlas	Update the A&A process to be consistent with NIST 300-37 and the Risk Management Framework	Updates required to ensure agency compliance.	Various

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
2	Bo Berlas	Inserted Roles and Responsibilities relating to A&A from the GSA IT Security Policy	Identify A&A Roles and Responsibilities	3
3	Bo Berlas	New implementation guidance for NIST 800-53 controls.	To facilitate implementation of required controls	25
4	Bo Berlas	New NIST 800-53 assessment test cases	Required to facilitate assessment of NIST 800-53 controls	Appendix C
5	Bo Berlas	New OCISO A&A Review SOP	Documents the process for submission of A&A packages to the OCISO and the detailed procedural steps performed by the OCISO to verify A&A compliance.	Appendix E
6	Bo Berlas	New guidance for A&A of Minor Systems	To facilitate assessment of minor systems.	22
		Revision 6 – December 16, 2010		
1	Bo Berlas	Updated references for Certification, Accreditation, and Certification and Accreditation (C&A) to Assessment, Authorization, and Assessment and Authorization (A&A), respectively.	To be consistent with the current terminology in NIST 800-37.	Throughout
2	Bo Berlas	Inserted guidance for forming sections 1-10 of the SSP for cloud computing system SSPs.	To address cloud specific security challenges.	12
		Revision 7 – May 31, 2011		
1	Bo Berlas	Updated references to A&A to security authorization process and authorization package or A&A package to security authorization package.	To be consistent with the current terminology in NIST 800-37.	Throughout
2	Bo Berlas	Inserted guidance for review of minimal impact SaaS solutions.	To document required review activities for such systems.	25
3	Bo Berlas	Updated Appendix E to include a revised OCISO Security Authorization Package Review SOP.	To reflect current version of the SOP.	48
		Revision 8 – November 25, 2015		
1	Lewis/ Sitcharing	Changes made throughout the document to reflect NIST and GSA requirements	Updated to reflect and implement the most current NIST 800-53-Rev4 and GSA requirements	Various
		Revision 9 – May 19, 2016		
1	Wilson/ Klemens	Restructuring of the document, modifications to specific process descriptions.	Updated to reflect current acceptance of risk process and rename Minor Application process to	Various

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
			Subsystem process and revise its description. Restructuring and editing throughout.	
		Revision 10 – April 10, 2017		
1	Desai/ Klemens	Clarifying system definitions and penetration testing requirements.	Included definitions of Federal and Contractor systems. Clarified when systems are required to have penetration tests as part of their assessment.	Sections 1.2, 4.1.7
2	Klemens	Update and edit document.	Updating of hyperlinks, editing of document, updates to align with other GSA documents.	Throughout
		Revision 11 – October 10, 2017		
1	Dean/ Feliksa/ Klemens	Update hyperlinks and minor editorial changes.	Hyperlinks were updated so outdated, superseded documents would not be provided. Minor edits to clarify current GSA processes.	Throughout
		Revision 12 – January 17, 2018		
1	Feliksa/ Klemens	Integrate the NIST Cybersecurity Framework (CSF), update A&A process and POA&M information, remove Cloud Controls.	Comply with Executive Order 13800, update processes based on revised procedures, streamline document by moving cloud controls.	Throughout
		Revision 13 – May 14, 2018		
1	Klemens	Added a provision for piloting new A&A processes. Updated Lightweight Security Authorization Process, MiSaaS, CSF content.	Allows a new A&A process to be piloted/tested. Align with revised GSA and NIST guidance.	Sections 1, 3.2.2, 3.2.6, Appendix A, Appendix C
		Revision 14 – February 1, 2019		
1	Klemens	Updated information on compliance/configuration scans. Updated hyperlink references. Added Program and Project Manager roles. Removed CTW as attachment to SSP.	Clarify GSA policy and guidance on compliance to hardening guides. Update to new format and style for hyperlinks. Added roles added to 2100.1. Data in the CTW is available in the SSP Template and Control Summary Table.	Throughout
2	Klemens	Added information concerning Binding Operational Directives (BOD) requirements and clarified encryption of data at rest requirements.	Clarify GSA policy and guidance on BOD and encryption requirements.	10, 12, 14, 38, 47

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
3	Klemens	Updated penetration testing requirements. Editing to align with current format, style, structure.	Provide the latest guidance on penetration testing requirements	34, 38, various
		Revision 15 – July 25, 2019		
1	Klemens	Updated SC-28 (1) control applicability and parameter. Revised references to BODs to Cybersecurity Directives which include BODs and Emergency Directives. Revised parameter for SI-2(3).	Updated GSA parameters and guidance on NIST controls.	Multiple
		Revision 16 – October 3, 2019		
1	Dean/Klemens	Revised to include/update information on Showstopper Controls, configuration compliance metric, vulnerability remediation timeframes, reference additional procedural guides, and add Certification Letter as part of security authorization process.	Updated to reflect additional Federal and GSA guidance and process changes.	Multiple
2	Klemens	Added PL-8 and SA-8 to the table of GSA required controls, removed LATO SSP/SAR/Test Cases from LATO process description and appendices.	Updated to reflect additional Federal and GSA guidance and process changes.	Multiple
		Revision 17 – July 1, 2020		
1	Dean/Klemens	Revisions include: • Retitled to "Managing Enterprise Cybersecurity Risk" • Included the GSA Risk Executive Function role • Added a requirement for independent assessment of common controls • Added Approval to Use (ATU) and GSA processes for ATUs • Added Leveraged FedRAMP Authorization to Operate (ATO) process • Updated ATO and control sections	Updated to reflect additional Federal and GSA guidance and process changes.	Multiple
		Revision 18 – September 11, 2020		
1	Desai/Klemens	Revisions include: • Added guidance on implementing, documenting, and assessing Cloud Service Provider (CSP) customer responsibilities.	Updated to reflect GSA guidance regarding customer responsibility controls.	Sections 5.3, 5.4, and 13

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
		• Updated Encryption of Sensitive Data information in Showstopper table.		
		Revision 19 – April 15, 2021		
1	Desai/Klemens/ Dean	Revisions include: • Incorporate NIST SP 800-37, Revision 2 • Incorporate NIST SP 800-53, Revision 5. • Update existing GSA A&A process descriptions. • Add Protecting CUI in Nonfederal Systems Assessment process. • Incorporate Clean ATO process, including update to A&A Package approval. • Add guidance on the use operational/live date in preproduction systems. • Incorporate Management Implementation Plan processes. • Update SAR and POA&M processes. • Update the FedRAMP XaaS section to include the requirement for assessments.	Incorporate updated NIST publications and GSA processes	Throughout
		Revision 20 – May 18, 2021		
1	Desai/Klemens	Revisions include: • Added SC-8/SC-8(1) controls to Showstoppers and GSA additional controls. • Added CISO and AO approval required before pursuing a 90-day LATO. • Added IPv6 transition requirement. • Revised scope to clarify requirement to adhere to all GSA security guides and requirements. • Clarification on determining the appropriate ATU/ATO process to follow.	Update showstopper controls, approval requirement to use 9-day LATO, IPv6 transition requirements, revise scope section, clarify identification of appropriate process for systems.	Multiple
		Revision 21 – July 21, 2021		
1	Desai/Klemens	Revisions include: • Added PE-8(3), PL-9, RA-8 as additional GSA controls.	Update additional NIST controls required by GSA, add requirement to provide FedRAMP PMO any ATO	Sections 4, 8, and 9

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
		• Added requirement that any ATO Letter leveraging a FedRAMP ATO must be provided to the FedRAMP PMO. • Editorial updates.	Letters leveraging FedRAMP authorizations, editorial updates.	
		Revision 22 – December 30, 2021		
1	Desai/Klemens	Revisions include: • Updated timeline for NIST SP 800-53A assessments to be completed. • Updated to reflect requirements per BOD 22-01 and ED 22-02, including adding to Showstoppers. • Updated AOR section to align with latest guidance. • Updated GSA CISO controls to reflect updates to 800-53 applicability and GSA guidance.	Updated to align with current Federal requirements, guidelines, and GSA guidance.	Throughout
		Revision 23 – May 9, 2022		
1	Desai/Klemens	Revisions include: • Updated timeline for NIST SP 800-53/53A SSPPs and assessments to be completed. • Updated parameter for NIST SP 800-53 Control RA-9. • Updated CISA KEV POA&M and AOR information. • Updated to current format and structure.	Updated to align with current GSA guidance.	Throughout

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

Approval

IT Security Procedural Guide: Managing Enterprise Cybersecurity Risk, CIO-IT Security-06-30, Revision 23, is hereby approved for distribution.

DocuSigned by:
Bo Berlas
FD717926161544F...

Bo Berlas
GSA Chief Information Security Officer

Contact: GSA Office of the Chief Information Security Officer (OCISO), Policy and Compliance Division (ISP), at ispcompliance@gsa.gov.

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

Table of Contents

1 Introduction 1
1.1 Purpose 3
1.2 Scope 3
1.3 Policy 4
1.4 GSA Archer GRC Implementation 4
1.4.1 Agency System Inventory 4
1.4.2 Authorization Packages 4
1.5 Assessment and Authorization Roles and Responsibilities 4
1.5.1 GSA Administrator 5
1.5.2 Risk Executive (Function) 5
1.5.3 GSA Chief Information Officer (CIO) 5
1.5.4 Chief Information Security Officer (CISO) 5
1.5.5 GSA Senior Agency Official for Privacy (SAOP) 5
1.5.6 GSA Chief Privacy Officer (CPO) 5
1.5.7 Heads of Services and Staff Offices (HSSOs) 6
1.5.8 Authorizing Officials (AOs) 6
1.5.9 Office of CISO Division Directors 6
1.5.10 Information Systems Security Managers (ISSMs) 6
1.5.11 Information Systems Security Officers (ISSOs) 6
1.5.12 System Owners 6
1.5.13 Program Managers 7
1.5.14 Project Managers 7
1.5.15 Data Owners (i.e., Functional Business Line Managers) 7
1.5.16 Contracting Officers (COs)/Contracting Officer's Representatives (CORs) 7
1.5.17 Custodians 7
1.5.18 Users of IT Resources 8
1.5.19 System/Network Administrators 8
2 Identifying Appropriate ATU or ATO Process 8
2.1 Identifying the Appropriate ATU Process 8
2.2 Identifying the Appropriate ATO Process 8
3 ATU Process Summaries 10
3.1 GSA Salesforce Platform Process 10
3.2 Federalist Site Process 10
3.3 RPA Process 10
3.4 Google Extensions and Add-ons 11
3.5 Google Apps Scripts 11
3.6 GCP Services 11
3.7 AWS Services 12
4 A&A Process Summaries 12
4.1 GSA Standard A&A Process 13
4.2 Lightweight Security Authorization Process 13
4.3 Low Impact Software as a Service (LiSaaS) Solutions Authorization Process 14
4.4 GSA Agency FedRAMP Process 14
4.5 Moderate Impact Software as a Service (MiSaaS) Security Authorization Process 15
4.6 GSA Subsystem Process 16
4.7 GSA Ongoing Authorization (OA) Program 16

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

4.8 GSA Leveraged FedRAMP XaaS Solution Process 17
5 GSA Standard A&A Process 18
5.1 RMF PREPARE Step 19
5.1.1 TASK P-1: Risk Management Roles 20
5.1.2 TASK P-2: Risk Management Strategy 20
5.1.3 TASK P-3: Risk Assessment – Organization 20
5.1.4 TASK P-4: Organizationally – Tailored Control Baselines and Cybersecurity Framework Profiles (OPTIONAL) 20
5.1.5 TASK P-5: Common Control Identification 20
5.1.6 TASK P-6: Impact-Level Prioritization (Optional) 21
5.1.7 TASK P-7: Continuous Monitoring Strategy – Organization 21
5.1.8 TASK P-8: Mission or Business Focus 22
5.1.9 TASK P-9: System Stakeholders 22
5.1.10 TASK P-10: Asset Identification 22
5.1.11 TASK P-11: Authorization Boundary 22
5.1.12 TASK P-12: Information Types 23
5.1.13 TASK P-13: Information Life Cycle 23
5.1.14 TASK P-14: Risk Assessment – System 23
5.1.15 TASK P-15: Requirements Definition 23
5.1.16 TASK P-16: Enterprise Architecture 24
5.1.17 TASK P-17: Requirements Allocation 24
5.1.18 TASK P-18: System Registration 24
5.2 RMF CATEGORIZE Step 24
5.2.1 TASK C-1: System Description 25
5.2.2 TASK C-2: System Categorization 25
5.2.3 TASK C-3: System Categorization Review and Approval 25
5.3 RMF SELECT Step 25
5.3.1 TASK S-1: Control Selection 25
5.3.2 TASK S-2: Control Tailoring 26
5.3.3 TASK S-3: Control Allocation 26
5.3.4 TASK S-4: Documentation of Planned Control Implementations 27
5.3.5 TASK S-5: Continuous Monitoring Strategy – System 27
5.3.6 TASK S-6: Plan Review and Approval 28
5.4 RMF IMPLEMENT Step 28
5.4.1 TASK I-1: Control Implementation 28
5.4.2 TASK I-2: Update Control Implementation 30
5.5 RMF ASSESS Step 30
5.5.1 TASK A-1: Assessor Selection 30
5.5.2 TASK A-2: Assessment Plan 31
5.5.3 TASK A-3: Control Assessments 32
5.5.4 TASK A-4: Assessment Reports 32
5.5.5 TASK A-5: Remediation Actions 33
5.5.6 TASK A-6: Plan of Action and Milestones 34
5.6 RMF AUTHORIZE Step 35
5.6.1 TASK R-1: Authorization Package 35
5.6.2 TASK R-2: Risk Analysis and Determination 36
5.6.3 TASK R-3: Risk Response 36
5.6.4 TASK R-4: Authorization Decision 36

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

5.6.5 TASK R-5: Authorization Reporting 37
5.7 RMF MONITOR Step 37
5.7.1 TASK M-1: System and Environment Changes 37
5.7.2 TASK M-2: Ongoing Assessments 38
5.7.3 TASK M-3: Ongoing Risk Response 38
5.7.4 TASK M-4: Authorization Package Updates 41
5.7.5 TASK M-5: Security and Privacy Reporting 41
5.7.6 TASK M-6: Ongoing Authorization 41
5.7.7 TASK M-7: System Disposal 42
5.8 A&A Guidance for Significant Changes 42
5.9 A&A Guidance for Expiring Authorizations 42
6 Protecting Confidential Unclassified Information (CUI) in Nonfederal Systems and Organizations 43
7 Independent Assessment of Enterprise-wide Common and Hybrid Controls 43
8 GSA Implementation of CA, PL, and RA Controls 44
8.1 Assessment, Authorization, and Monitoring (CA) 44
8.1.1 CA-1 Policy and Procedures 44
8.1.2 CA-2 Control Assessments 45
8.1.3 CA-3 Information Exchange 46
8.1.4 CA-5 Plan of Action and Milestones 47
8.1.5 CA-6 Authorization 48
8.1.6 CA-7 Continuous Monitoring 49
8.1.7 CA-8 Penetration Testing 51
8.1.8 CA-9 Internal System Connections 52
8.2 Planning (PL) 52
8.2.1 PL-1 Policy and Procedures 52
8.2.2 PL-2 System Security and Privacy Plans 53
8.2.3 PL-4 Rules of Behavior 55
8.2.4 PL-8 Information Security Architecture 56
8.2.5 PL-9 Central Management 56
8.2.6 PL-10 Baseline Selection 57
8.2.7 PL-11 Baseline Tailoring 57
8.3 Risk Assessment (RA) 57
8.3.1 RA-1 Policy and Procedures 57
8.3.2 RA-2 Security Categorization 58
8.3.3 RA-3 Risk Assessment 59
8.3.4 RA-5 Vulnerability Monitoring and Scanning 60
8.3.5 RA-7 Risk Response 62
8.3.6 RA-8 Privacy Impact Assessments 62
8.3.7 RA-9 Criticality Analysis 63
9 Additional NIST Controls Required by GSA 64
10 Summary 67

Appendix A: CSF Function, Category, and Subcategory Definitions 68
Appendix B: Consolidated List of Guidance, Policies, Procedures, Templates 76
Appendix C: A&A Process Package Document Lists/Links 79
Appendix D: GSA Defined Cloud Controls 83
Appendix E: Scanning Frequency By A&A Process 84
Appendix F: Showstopper Capabilities and Associated Controls 85

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

Figure 5-1. Risk Management Framework Steps (from NIST 800-37, Revision 2) Error! Bookmark not defined.

Table 2-1. GSA ATU Processes 8
Table 2-2. GSA ATO Processes 9
Figure 5-1. Risk Management Framework Steps (from NIST 800-37, Revision 2).....18
Table 9-1: GSA Additional NIST Control Requirements 64
Table A-1: NIST CSF Functions Mapped to NIST SP 800-37 RMF Steps.....69
Table A-2: CSF Category/Subcategory Definitions.....71
Table F-1: GSA Showstopper Capabilities/Controls.....85

NOTE: Hyperlinks in this guide are provided as follows:

- Appendix B - Consolidated List of Guidance, Policies, Procedures, Templates. This appendix contains hyperlinks to Federal Regulations/Guidance and to GSA web pages containing GSA policies, guides, and forms/templates.
- In running text - Hyperlinks will be provided if they link to a location within this document (i.e., a different section or an appendix). Hyperlinks will be provided for external sources unless the hyperlink is to a web page or document listed in Appendix B. For example, Google Forms, Google Docs, and websites will have links.
- It may be necessary to copy and paste hyperlinks in this document (Right-Click, Select Copy Hyperlink) into a web browser rather than using Ctrl-Click to access them.

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

1 Introduction

The General Services Administration (GSA) uses two approaches to permit information systems, applications, services, features, or functions to be used.

- Authorization to Operate (ATO) - An official management decision authorizing the operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation.
- Approval to Use (ATU) – A risk-based approval process for usage of services, features, or functions on information systems or platforms with an existing ATO.

Security Assessment and Authorization (A&A) processes within the GSA lead to an ATO and are based on the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) and the security authorization process as described in NIST Special Publication (SP) 800-37, Revision 2, "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy." This guide describes key activities in managing enterprise-level cybersecurity risk through a system life cycle perspective including information system ATO and continuous monitoring. Every GSA Information Technology (IT) system/platform must use one of the A&A processes identified in this guide or a pilot process as described later in this section.

In Appendix F, Table F-1, GSA has identified a list of Showstopper capabilities and NIST SP 800-53 controls associated with them, including compliance with Binding Operational Directive (BOD) 22-01 and Emergency Directive (ED) 22-02. Showstoppers and controls associated with them, if not fully compliant, will keep a system from receiving a full ATO.

NIST SP 800-53, Revision 5, "Security and Privacy Controls for Information Systems and Organizations," and NIST SP 800-53B, "Control Baselines for Information Systems and Organizations," were published on December 10, 2020. NIST SP 800-53A, Revision 5, "Assessing Security and Privacy Controls in Information Systems and Organizations," became final on January 25, 2022. GSA has established the following timelines for systems to have System Security and Privacy Plans (SSPPs) prepared and assessments conducted in accordance with the NIST documents using GSA templates.

The GSA approach to the Rev. 5 transition is risk based; considerate of the level of effort required to update, assess, and authorize the new R5 controls; and, reflective of the FedRAMP Rev. 5 Transition timelines. FedRAMP is expected to release the Final Rev5 Baselines in FY22Q4 with the goal of transitioning all CSPs with updated documentation and assessment by FY23Q4.

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

Group	Revision 5 Updates Required, Assessment Complete and New ATO		
	SSPPs Updated	Assessment Complete and New ATO	Comment
Group A – Federal Information Process Standard (FIPS) 199 High Impact Systems, High Value Assets (HVAs), and Government Wide Shared Services Systems on this list.	12/10/2021	1/25/2023	Within 1 year of the release of NIST SP 800-53A Delta (including showstoppers) or Full Assessment
Group B – Systems in GSA's Ongoing Authorization (OA) Program	10/15/2022	9/30/2023	Delta assessment (including showstoppers)
Group C – GSA systems not in any other group.	10/15/2022	System's next scheduled 3-year assessment	Full assessment
Group D – FedRAMP Leveraged XaaS	SSPP Updated, Assessed, and Authorized within 12 months of the Cloud Service Provider's (CSP) FedRAMP Rev. 5 Transition		CSP identified Customer Responsible Controls (CRM)
Group E – FedRAMP Sponsored CSPs	SSPP Updated, Assessed, and Authorized per FedRAMP PMO requirements and timelines		Per FedRAMP Requirements

GSA may conduct pilots of additional A&A processes when a system or the evolving IT and IT security environments indicate a process different from any of GSA's existing processes is preferred. Piloting of new processes must be coordinated with the GSA Chief Information Security Officer (CISO). Final approval of the process is indicated by the CISO concurring with any ATO resulting from the pilot.

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

ATU processes and procedures are based on evaluating the risk of using available services, features, or functions based on their characteristics and environment. Section 3 provides additional information on GSA's ATU processes.

Any deviations from the security requirements established in GSA Order CIO 2100.1, "GSA Information Technology (IT) Security Policy" must be coordinated by the Information Systems Security Officer (ISSO) through the appropriate Information Systems Security Manager (ISSM) and authorized by the Authorizing Official (AO). Any deviations, exceptions, or other conditions not following GSA policies and standards must be submitted using the Security Deviation Request Google Form.

Executive Order (EO), EO 13800, "Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure" requires all agencies to use "The Framework for Improving Critical Infrastructure Cybersecurity (the Framework) developed by the NIST or any successor document to manage the agency's cybersecurity risk." This NIST document is commonly referred to as the Cybersecurity Framework (CSF). The CSF complements, and does not replace, an organization's risk management process and cybersecurity program. GSA uses NIST's RMF as its foundation for managing risk. Further information on how the CSF relates to GSA's use of the NIST RMF is explained in Section 5 and Appendix A where the CSF categories and subcategories are defined.

1.1 Purpose

This procedural guide defines the GSA cybersecurity risk management process. It addresses the security authorization processes GSA has implemented for information systems to obtain an ATO. This guide identifies ATU processes for services, features, and functions to be used at GSA, and the process for protecting Confidential Unclassified Information (CUI) in nonfederal systems. The guide describes the key activities in managing enterprise-level cybersecurity risk as described in NIST SP 800-37. This guide assists agency and contractor personnel to understand and fulfill their security responsibilities regarding ATO, ATU, and other processes.

1.2 Scope

The requirements outlined within this guide apply to all GSA Federal employees, contractors, and vendors who oversee/protect GSA information systems and data. The guide provides GSA Federal employees, contractors, and vendors as identified in CIO 2100.1, and other IT personnel involved in performing A&A activities, the specific processes to follow for properly accomplishing cybersecurity activities. All GSA systems must adhere to one of the processes described in this guide, the security requirements specified in CIO 2100.1, and the guides listed on the IT Security Technical Guides and Standards and Procedural Guides web pages. The following definitions are provided for classifying information systems/platforms within the scope of this guide.

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

- **Contractor System.** An information system in GSA's inventory processing or containing GSA or Federal data where the infrastructure and applications are wholly operated, administered, managed, and maintained by a contractor in non-GSA facilities.
- **Federal System (i.e., Agency System).** An information system in GSA's inventory processing or containing GSA or Federal information where the infrastructure and/or applications are NOT wholly operated, administered, managed, and maintained by a Contractor.

1.3 Policy

As detailed within CIO 2100.1, Authorizing Officials (AO) must ensure risk assessments are performed as part of A&A activities before a system is placed into production, when significant changes are made to the system, and as specified in this guide and the guides for GSA's other A&A processes.

1.4 GSA Archer GRC Implementation

GSA has implemented its official agency system inventory in Archer GRC. GSA is in the process of implementing authorization packages for its system inventory using Archer GRC's A&A module. As GSA continues its Archer implementation, specific activities described in the guide will be incorporated in Archer to take advantage of its automation capabilities. Any questions regarding the use of Archer GRC at GSA should be sent to archersupport@gsa.gov.

1.4.1 Agency System Inventory

The agency system inventory in Archer GRC contains attributes such as responsible organization, system name, FIPS security categorization level, ATO type, and ATO date. The inventory includes an A&A repository for storing all system A&A documents and artifacts for GSA systems.

1.4.2 Authorization Packages

Authorization packages have been created in Archer GRC for GSA's systems and the task of implementing the authorization process for systems is just starting. The first steps in this process include inputting security categorization, privacy, and system demographics (boundary, connections, etc.) into Archer GRC, and allocating NIST SP 800-53 security controls. Future steps include conducting assessments, managing plans of action and milestones (POA&Ms), and the entire A&A process in Archer GRC.

1.5 Assessment and Authorization Roles and Responsibilities

There are many roles associated with the security authorization process. System Owners for each information system are responsible for ensuring their respective Service/Staff Office (S/SO) systems have been through the GSA A&A process, have received an ATO from the AO, and received concurrence from the GSA Office of the CISO (OCISO). The complete roles and responsibilities for agency management officials and others with significant IT Security

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

responsibilities are defined fully in Chapter 2 of CIO 2100.1. The following sections provide a high-level description of the responsibility for the primary roles with management and operational A&A responsibilities.

1.5.1 GSA Administrator

The GSA Administrator is responsible for ensuring an information security program is developed, documented, and implemented to provide security for all systems, networks, and data that support the operations of GSA.

1.5.2 Risk Executive (Function)

The Risk Executive (Function) at GSA is handled by the Enterprise Management Board (EMB), chaired by the Deputy Administrator who is also the Senior Accountable Official for Risk Management (SAORM). For cybersecurity risks, the Enterprise Risk Executive Subcommittee (ERES), co-led by the Deputy Performance Improvement Officer and the CISO, identifies and monitors agency-wide risks and ensures the EMB is updated on the risks and impacts to GSA. The CISO, Authorizing Officials, and subject matter experts facilitate the consistent application of cybersecurity risk management across GSA.

1.5.3 GSA Chief Information Officer (CIO)

The GSA Chief Information Officer (CIO) has overall responsibility for the GSA IT Security Program. The CIO is responsible for providing guidance, assistance, support, and management processes to GSA staff and organizations to enable them to perform their responsibilities with regard to GSA's IT Security Program.

1.5.4 Chief Information Security Officer (CISO)

Public Law 113-283, "Federal Information Security Modernization Act of 2014" (FISMA), establishes the designation of a senior agency information security officer responsible for complying with Federal security requirements. GSA has assigned this role to the CISO. The CISO is the focal point for all GSA IT security and must ensure the security requirements described in this Order are implemented agency wide. The CISO reports directly to the CIO as required by FISMA.

1.5.5 GSA Senior Agency Official for Privacy (SAOP)

The SAOP is responsible for ensuring GSA's compliance with privacy laws, regulations and GSA policy, and the privacy control baseline in NIST SP 800-53. Within GSA, the CIO has designated the Deputy CIO as the SAOP.

1.5.6 GSA Chief Privacy Officer (CPO)

The CPO is responsible for overseeing GSA's Privacy Program whose mission it is to preserve and enhance privacy protections for all individuals whose personal information is handled by GSA and to encourage transparency of GSA operations involving personal information. The CPO manages GSA's Privacy Act Program and administers GSA's compliance with privacy laws and

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

regulations. The CPO is responsible for developing, managing, and administering GSA's Privacy Program Plan and Privacy Strategy Plan.

1.5.7 Heads of Services and Staff Offices (HSSOs)

HSSOs are responsible for authorizing the operation of all systems, networks, and applications for which they have responsibility. They may delegate some of their authority (e.g., the role of Authorizing Official in writing) to appropriately qualified individuals within their organizations.

1.5.8 Authorizing Officials (AOs)

AOs are responsible for authorizing the operation of all systems, networks, and applications for which they have responsibility. They may delegate some of their authority (e.g., the role of Authorizing Official in writing) to appropriately qualified individuals within their organizations.

1.5.9 Office of CISO Division Directors

OCISO Directors are the intermediary to the AO for ensuring IT security is properly implemented. The Director is the focal point for all IT system security matters for the IT resources under their responsibility.

1.5.10 Information Systems Security Managers (ISSMs)

ISSMs report to the ISSO Support Division (IST) Director in the OCISO. There is at least one ISSM per AO. The ISSM is responsible for all IT system security and privacy matters for the systems under their authority. ISSMs work with ISSOs, System Owners, AOs, and others as security and privacy controls are implemented and review A&A packages for systems under their purview. ISSMs are appointed, in writing, by the Director of IST with concurrence by the CISO. An individual appointed as an ISSM for a system cannot also be assigned as the ISSO for the same system.

1.5.11 Information Systems Security Officers (ISSOs)

ISSOs are responsible for ensuring implementation of adequate system security and privacy protections, including proper control implementations, in order to manage cybersecurity risk aligned with the NIST CSF functions of Identify, Protect, Detect, Respond, and Recover. An ISSO must be assigned for every information system. An ISSO may have responsibility for more than one system, provided there is no conflict. An individual assigned as the ISSO for a system cannot also be the ISSM for the same system. ISSOs must be appointed via a designation letter. An ISSO must be knowledgeable of the information and processes supported by their assigned systems. ISSOs review A&A packages for systems under their purview.

1.5.12 System Owners

System Owners are management officials within GSA who bear the responsibility for the acquisition, development, maintenance, implementation, and operation of GSA's IT systems. System Owners represent the interests of the system throughout its lifecycle. Primary responsibility for managing risk rests with the System Owners. System Owners must ensure

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

their systems and the data each system processes have the necessary security and privacy controls in place and are operating as intended and protected IAW GSA regulations and any additional guidelines established by the OCISO and relayed by the ISSO or ISSM.

1.5.13 Program Managers

Program Managers are management officials within GSA who are responsible for developing, implementing, and/or overseeing multi-year IT initiatives that must be carried out through multiple related projects. A Program Manager focuses on the strategic goals of GSA. Program Managers are responsible for ensuring cyber risk is adequately managed and resources are allocated, monitored, and managed to support the required level of security for projects under their purview.

1.5.14 Project Managers

Project Managers are management officials within GSA who are responsible for managing a project within a larger program. A Project Manager is responsible for ensuring cyber risk is adequately managed and the schedule, resources, and tasks within a project include delivering security.

1.5.15 Data Owners (i.e., Functional Business Line Managers)

Data Owners are responsible for determining the security categorization level of systems based upon FIPS Publication 199, “Standards for Security Categorization of Federal Information and Information Systems,” and ensuring System Owners are aware of the sensitivity of data (e.g., Personally Identifiable Information, Controlled Unclassified Information) to be handled. They must coordinate with System Owners, ISSMs, ISSOs, and Custodians to ensure the data is properly stored, maintained, protected, and monitored IAW GSA policies, regulations and any additional guidelines established by GSA.

1.5.16 Contracting Officers (COs)/Contracting Officer’s Representatives (CORs)

COs/CORs are responsible for coordinating and collaborating with the CISO or other appropriate officials to ensure all agency contracts and procurements are compliant with the agency’s information security policy. They also must ensure the appropriate security and privacy contracting language is incorporated in each contract and task order.

1.5.17 Custodians

Custodians own the hardware platforms and equipment on which the data is processed. They are the individuals in physical or logical possession of information from Data Owners. They must coordinate with Data Owners and System Owners to ensure the data is properly stored, maintained, and protected.

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

1.5.18 Users of IT Resources

Authorized users of GSA IT resources, including all Federal employees and contractors, either by direct or indirect connections, are responsible for complying with GSA's IT Security Policy and procedures.

1.5.19 System/Network Administrators

System/Network Administrators are responsible for ensuring the appropriate security requirements are implemented consistent with GSA IT security policies and hardening guidelines.

2 Identifying Appropriate ATU or ATO Process

The next two sections list GSA's ATU and ATO processes along with applicability/qualifying criteria to use a specific process. The applicability/qualifying criteria listed in Tables 2-1 and 2-2 identify the conditions under which each process may be used. If additional guidance is necessary or there is a question about which process to use, contact any GSA ISSM, the IST, ISP, or ISE Directors, to determine the appropriate process to follow.

2.1 Identifying the Appropriate ATU Process

Table 2-1 identifies the applicability/qualifying criteria for GSA's ATU processes.

Table 2-1. GSA ATU Processes

ATU Process	Applicability/Qualifying Criteria
GSA Salesforce Platform (See Section 3.1)	• Applications that integrate into GSA's Salesforce Force.com platform and are hosted on Salesforce.com's infrastructure. • Applications developed for internal and external GSA use published on the GSA's Salesforce Force.com platform.
Federalist Site Review (See Section 3.2)	• Sites requesting to be hosted on the Federalist platform.
Robotic Process Automation (RPA) (See Section 3.3)	• Bots used to interact with GSA systems.
Google Extensions and Add-ons (See Section 3.4)	• Google Chrome browser extensions for use within GSA.
Google Apps Scripts (See Section 3.5)	• Google Apps scripts for use within GSA.
Google Cloud Platform (GCP) Services (See Section 3.6)	• Google Cloud Platform (GCP) services not currently Federal Risk and Authorization Management Program (FedRAMP) approved.
AWS Services (See Section 3.7)	• Amazon Web Services (AWS) services not currently FedRAMP approved.

2.2 Identifying the Appropriate ATO Process

Table 2-2 identifies the applicability/qualifying criteria for GSA's ATO processes.

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

Table 2-2. GSA ATO Processes

ATO Process	Applicability/Qualifying Criteria
GSA Standard A&A (See Section 5)	• All new and existing GSA information systems that do not fall under one of the other A&A processes.
Lightweight Security Authorization (See Section 4.2)	• New GSA information systems pursuing an agile development methodology. • Reside on infrastructures that have a GSA ATO concurred to by the CISO or a FedRAMP ATO. • Must be FIPS 199 Low or Moderate. • Prior to pursuing a 90-day Limited Authorization to Operate (LATO) the GSA CISO and AO must approve the use of the process.
Low Impact Software as a Service (LiSaaS) Solutions Authorization Process (See Section 4.3)	• Cloud computing Software as a Service (SaaS) solutions that are implemented within GSA. • Data already exists in the public domain or data is non-sensitive and is considered FIPS 199 Low impact. • GSA would be caused limited harm regardless of the consequence of an attack or compromise. • Dollar cost for such deployments do not exceed $100,000 annually • A disruption in service or the inability to access the service will not have an impact to operations or business process. • Risk level of the LiSaaS solution will be determined through completion of a SaaS Solution Profile.
GSA Agency FedRAMP (See Section 4.4)	• A CSP requesting GSA Agency sponsorship into FedRAMP. • GSA accepts sponsoring the CSP. • GSA determines CSP's security authorization package will be considered FedRAMP compliant.
Moderate Impact Software as a Service (MiSaaS) Security Authorization (See Section 4.5)	• New GSA information systems pursuing an agile development methodology. • Reside on infrastructures that have, or are pursuing, a Federal Risk and Authorization Management Program (FedRAMP) provisional ATO. • Must be FIPS 199 Moderate.
GSA Subsystem (See Section 4.6)	• Classified as a subsystem (and not a Salesforce application). • Dependent upon resources provided by its supporting FISMA system. • FIPS 199 Low or Moderate. • FIPS 199 level may be equal to or below the level of the supporting FISMA system.
GSA Ongoing Authorization (OA) Program (See Section 4.7)	• The information system must have had all of its NIST SP 800-53 security controls for its applicable FIPS 199 level, and any additional controls required by the GSA CISO assessed within the past 18 months and issued an ATO. • The information system must have deployed GSA's enterprise ISCM tools, based on applicable system requirements, defined within the GSA ISCM Enterprise Security Management Tools.
GSA Leveraged FedRAMP XaaS Solution (See Section 4.8)	• Leveraged XaaS must have a FedRAMP ATO. • All customer responsibilities in the CSP's Customer Responsibility Matrix (CRM) must be addressed in a CRM SSP.

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

3 ATU Process Summaries

Additional details about the GSA ATU processes listed in Table 3-1 are provided in the following sections.

3.1 GSA Salesforce Platform Process

- **Document Reference:** IT Security Procedural Guide: Salesforce Platform Security Implementation (CIO-IT Security-11-62)
- **Result:** Salesforce Application ATU
- **Summary of Process**: Specific to applications developed for internal and external GSA use published on GSA's Salesforce Force.com platform. Applications are approved for use based on implementation of NIST SP 800-53 controls, security configuration settings, and user permissions as detailed in CIO-IT Security-11-62.
- **Approval Process**: After the ISSM accepts/approves the ATU package it becomes a part of the SSPP and allows the minor application to be added to the Salesforce inventory along with POAMs reflecting any identified vulnerabilities.

3.2 Federalist Site Process

- **Document Reference**: IT Security Procedural Guide: Federalist Site Review and Approval Process (CIO-IT Security-20-106).
- **Result**: Federalist Site ATU
- **Summary of Process**: Each site requesting to be on-boarded to the Federalist for hosting must complete a Federalist Site Review and Approval template, available on the InSite Forms and Aids page. Site URLs must be scanned in accordance with GSA's NSP 800-53 control RA-5, Vulnerability Scanning, as described in CIO-IT Security-18-90.
- **Approval Process**: The ISSO and Site Owner complete the Federalist Site Review and Approval template and the Federalist ISSM reviews for approval.

3.3 RPA Process

- **Document Reference**: IT Security Procedural Guide: Robotic Process Automation (RPA) Security (CIO-IT Security-19-97).
- **Result**: RPA ATU
- **Summary of Process**: Each request to approve a GSA RPA Bot must include a completed RPA Attributes Questionnaire template, available on the InSite Forms and Aids page. The questionnaire includes questions/requirements based on the type of bot (i.e., simple, complex), rules of behavior, and interaction with systems.

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

- **Approval Process**: After reviewing the questionnaire and required artifacts, the RPA ISSO may approve simple bots. After review, the RPA ISSM relays the questionnaire and artifacts for complex bots to the RPA ISSM for approval.

3.4 Google Extensions and Add-ons

- **Document Reference**: Google Extensions and Add-Ons InSite page
- **Result**: Addition to the lists of GSA Approved/Rejected Extensions or Add-ons
- **Summary of Process**: Each request for a Google Extension or Add-on must follow the process described on the Requesting Google Add-Ons and Google Chrome Extension Request InSite web pages. Requests for new extensions or add-ons (i.e., not already approved or rejected) require a Service Catalog request.
- **Approval Process**: Service Catalog requests for new extensions and add-ons are routed to the ISE Division for review. After ISE completes the review, the approved/rejected lists are updated and the requestor notified along with rationale if rejected.

3.5 Google Apps Scripts

- **Document Reference**: GSA Order 2100.1, Chapter 4, Policy for Protect Function, Section mm
- **Result**: Google App Script ATU
- **Summary of Process**: Internally developed scripts are implicitly allowed but require review by the ISE Division and may be restricted from use pending the results of the ISE review. Internally developed scripts must follow the GSA naming convention as described in GSA Order CIO 2100.1. Externally developed scripts are prohibited but may be allowed following OCISO review.
- **Approval Process**: Use the Google App Script Approval Form to request approval for internal and external scripts. After ISE completes its review, the script will be approved/rejected and the requestor notified along with rationale if rejected.

3.6 GCP Services

- **Document Reference**: CIO-IT Security Procedural Guide being developed, in the interim contact seceng@gsa.gov for information
- **Result**: GCP (Non-FedRAMP) Services ATU
- **Summary of Process**: Specific to GCP services not currently FedRAMP approved. Requestors must provide the following details to ISE in order to request GCP services:
  - GCP Service Type;
  - GCP Service Name;

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

  - Service Namespace;
  - Short Service Description; and
  - Service Description.
- **Approval Process**: Requests for GCP services to be reviewed should be submitted to seceng@gsa.gov. ISE will approve or reject the GCP service based on a security review of the service. Approved services may require additional usage conditions/restrictions for use at GSA.

3.7 AWS Services

- **Document Reference**: ISE Master AWS Services Tracking List (see About This Sheet Tab)
- **Result**: AWS (Non-FedRAMP) Services ATU
- **Summary of Process**: Specific to AWS services not currently FedRAMP. Requestors must provide the following details to ISE in order to request AWS services:
  - AWS Service Description;
  - AWS Service Name; and
  - Core Security Information (see ISE AWS Service Template for details)
- **Approval Process**: Requests for AWS services to be reviewed should be submitted to seceng@gsa.gov. ISE will approve or reject the AWS service based on a security review of the service. Approved services may require additional usage conditions/restrictions for use at GSA.

4 A&A Process Summaries

GSA's different A&A processes have been developed to ensure the risks to operating GSA IT systems and their data are reduced to the extent possible based on budget constraints, business requirements and other resource issues. For all A&A processes (except for a 90-day LATO) before assessment activities for an information system can begin, the following requirements must be met:

(1) The information system must be clearly defined in an SSPP or LiSaaS Survey/Checklist.
(2) The information system's architecture must be approved by the OCISO Security Engineering Division (ISE).
(3) A SAP (or other method of assessment when a SAP is not required) must be approved.

To assist ISSOs and/ISSMs in managing recurring tasks regarding A&A processes and the security of GSA information systems Federal and Contractor ISSO Checklists have been developed in GSA's implementation of Archer GRC.

Additional details about the GSA ATO processes listed in Table 2-2 are provided in the following sections. In addition, GSA is developing IT Security Procedural Guide CIO-IT Security-21-114: Clean Authorization to Operate (ATO) to provide a clearly defined, phased approach for successfully completing an A&A and receiving an ATO for a system. The Clean ATO guide

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

includes links to standard operating procedures (SOPs) that provide additional details regarding executing tasks that occur prior to assessments, during assessments, and after assessments to ensure systems can effectively and efficiently receive an ATO.

Any GSA system leveraging a FedRAMP authorization must provide a copy of the GSA ATO Letter to the FedRAMP Program Management Office (PMO). ISSOs must coordinate with their ISSM to ensure the FedRAMP PMO receives notification.

4.1 GSA Standard A&A Process

- **Document Reference**: Section 5 of this guide.
- **Result**: Full 3 Year ATO.
- **Summary of Process**: All new and existing GSA information systems must undergo a security A&A at least every three (3) years or whenever there is a significant change to the system's security posture. The result is an ATO for a period not to exceed three (3) years. Specific requirements are detailed throughout this guide.
- **Approval Process**: Follows the process described in Section 5.6.4, Authorization Decision.

4.2 Lightweight Security Authorization Process

- **Document Reference:** IT Security Procedural Guide: Lightweight Security Authorization Process (CIO-IT Security-14-68).
- **Result:** LATO - 90 day (Sprint or Standard)/1 Year (Moderate); Full 3 Year ATO (Low).
- **Summary of Process:** New GSA information systems pursuing an agile development methodology AND residing on infrastructures that have a GSA ATO concurred by the GSA CISO or a FedRAMP ATO. The process supports the following ATOs. Prior to pursuing a 90-day LATO the GSA CISO and AO must approve the use of the process.

  A 90-day LATO can be issued based on the results of a limited assessment (e.g., vulnerability scans, penetration tests). The following documents are required to issue a 90-day LATO:

  - Assessment Test Report (i.e., Enhanced Scanning and Assessment, Penetration)
  - POA&M
  - Certification Memorandum
  - ATO Letter.

  A one-year LATO (for FIPS 199 Moderate) or a three-year full ATO (for FIPS 199 Low) can be issued based on completing the process described in CIO-IT Security-14-68. The following documents are required:

  - System Security and Privacy Plan (with appendices/attachments)

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

- Security Assessment Report (with appendices/attachments)
- POA&M
- CRM
- Certification Memorandum
- ATO Letter.

- **Approval Process**: Follows the process described in Section 5.6.4, Authorization Decision.

4.3 Low Impact Software as a Service (LiSaaS) Solutions Authorization Process

- **Document Reference:** IT Security Procedural Guide: Low Impact Software as a Service (LiSaaS) Solutions Authorization Process (CIO-IT Security-16-75).

- **Result:** One year if the application is determined to be Low Risk, or up to three years if the application is determined to be a commodity, ancillary service that presents Very Low/Negligible risk.

- **Summary of Process:** Process is for cloud computing Software as a Service (SaaS) solutions that (1) are implemented for a limited duration; (2) involve data already in the public domain or data that is non-sensitive and could be considered FIPS 199 low impact; (3) could cause limited harm to GSA regardless of the consequence of an attack or compromise; (4) the dollar cost for such deployments do not exceed $100,000 annually; and (5) a disruption in service or the inability to access the service will not have an impact to operations or business process.

  A LiSaaS Solution Review Checklist template available on the InSite IT Security Forms and Aids page must be completed for all systems. An analysis of risk is performed based on the completed checklist. Very Low/Negligible risk solutions require a LiSaaS Solution Profile (also available at the preceding link) be completed; low risk solutions require the vendor to obtain a FedRAMP Tailored ATO. Detailed information is available in CIO-IT Security-16-75.

- **Approval Process**: Follows the process described in Section 5.6.4, Authorization Decision.

4.4 GSA Agency FedRAMP Process

- **Document Reference:** CSP Authorization Playbook-Getting Started with FedRAMP, additional details available in the FedRAMP Security Assessment Framework and FedRAMP General Document Acceptance Criteria

- **Result:** FedRAMP ATO (Agency)

- **Summary of Process:** A CSP may elect to request an Agency FedRAMP ATO from GSA. It is at the discretion of GSA to accept or deny the CSP's request for sponsorship. CSPs

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

which GSA agrees to sponsor for a FedRAMP authorization are required to follow the FedRAMP PMO authorization process requirements. GSA has defined assignments for NIST SP 800-53 control parameters within the FedRAMP Low and Moderate baselines as its organizationally defined parameters. The parameters are contained in GSA's Control Tailoring Workbook. Additional information about FedRAMP is available in the reference documents and at the FedRAMP webpage. The CSP must provide a security authorization package to GSA. If GSA determines the package to be FedRAMP compliant, the CSP in cooperation with GSA will pursue a FedRAMP ATO.

System Owners/AOs with questions about leveraging the FedRAMP security authorization process (to attain a Government wide authorization) should contact the OCISO at ispcompliance@gsa.gov.

- **Approval Process**: Follows the FedRAMP process.

4.5 Moderate Impact Software as a Service (MiSaaS) Security Authorization Process

- **Document Reference:** IT Security Procedural Guide: Moderate Impact Software as a Service (MiSaaS) Security Authorization Process (CIO-IT Security-18-88) describes the process and requirements for authorizing the operation of MiSaaS solutions within GSA.
- **Result:** 1 Year ATO
- **Summary of Process:** New GSA information systems pursuing an agile development methodology AND residing on infrastructures that have, or are pursuing, a FedRAMP provisional ATO. The process allows for a FIPS 199 Moderate impact SaaS to be granted a one-year ATO after completing the tailored RMF process detailed in CIO-IT Security-18-88.

  The following documents are required as part of the A&A Package:

  - MiSaaS SSPP
  - SAR, including
    - MiSaaS Test Workbook
    - OS (including DB), Web App scan data (as appropriate)
    - Penetration Test Report
  - POA&M
  - CRM
  - Certification Memorandum
  - ATO Letter

- **Result:** 1 Year ATO
- **Approval Process:** Follows the process described in Section 5.6.4, Authorization Decision

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

4.6 GSA Subsystem Process

- **A&A Process Reference:** Described within this section.
- **Result:** ATO aligned with subsystem's supporting FISMA system.
- **Summary of Process:** This process is specific to subsystems (other than Salesforce applications) which are: (1) categorized with a FIPS 199 security impact level of Low or Moderate; and (2) are dependent upon the resources provided by its underlying supporting FISMA system. The supporting FISMA system must be shown to provide a foundational level of protection for the subsystem; the subsystem may have a FIPS 199 level equal to or below the level of its supporting FISMA system.

  Subsystems with a FIPS 199 security impact level of Low will adhere to and implement the controls per CIO-IT Security-14-68: Lightweight Security Authorization Process.

  Subsystems with a FIPS 199 security impact level of Moderate will document all security and privacy controls where the subsystem has either hybrid or system specific requirements in an SSPP. These controls will be assessed using GSA's NIST 800-53 Test Cases and the results shared with the supporting FISMA system's System Owner/ISSO. All subsystems will be identified in Appendix C of their supporting FISMA system's SSPP which will also be attached to the hosting/supporting system's ATO Letter. All subsystems inherit its supporting FISMA system's ATO cycle.
- **Approval Process**: New and transferred subsystems receive an ATO based on the A&A process (see Summary Process description above) followed. Existing subsystems (and new and transferred when added) are included in the A&A Package review and approval process of their supporting FISMA system.

4.7 GSA Ongoing Authorization (OA) Program

- **A&A Process Reference:** IT Security Procedural Guide: Information Security Continuous Monitoring (ISCM) Strategy & Ongoing Authorization (OA) Program, CIO-IT Security-12-66.
- **Result:** Ongoing Authorization to Operate (OATO)
- **Summary of Process:** GSA has implemented its OA Program as summarized below.
  - A system must meet the OA prerequisites identified in CIO-IT Security-12-66.
  - An OA Checklist is completed by the OA Team in collaboration with the ISSO, ISSM, and system team. The OA checklist reviews five main security areas including ISCM/CDM Tools, Vulnerability Management, Configuration Compliance, Critical Security Controls and Security Documentation.
  - An Onboarding Assessment Report (OAR) is prepared by the OA Team and ISSO. The OAR is functionally the SAR for systems entering the OA Program.

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

  - Systems suitable for OA have an Onboarding Approval Meeting (OAM) held with the OA Team and system personnel.
  - OATO Letter is prepared and routed for signature.
  - Systems in OA undergo biannual performance metric reviews (PMRs) with results presented to the CISO and AO to make a risk-based determination on continuance in the OA program. Additional details are available in CIO-IT Security-12-66.

- **Approval Process**: Follows the same process described in Section 5.6.4, Authorization Decision, with the following exception, the Director of ISP replaces the Director of IST.

4.8 GSA Leveraged FedRAMP XaaS Solution Process

- **A&A Process Reference:** Described within this section.

- **Result:** ATO for a Leveraged FedRAMP XaaS Solution

- **Summary of Process:** GSA's process for issuing an ATO leveraging a FedRAMP XaaS is as described below. Every instance of a leveraged solution needs its own ATO unless the ATO is for an GSA enterprise solution.

  - A CRM SSPP is developed documenting the leveraged solution and GSA's implementation of the customer responsibilities listed in the CSP CRM for the solution. **Note:** The CRM SSPP is organized by customer responsibilities and not individual controls. A CRM SSPP Template is available on the InSite Forms and Aids page. The SSPP template includes as required attachments:
    - FIPS 199 Security Categorization identifying the information types GSA will use with the leveraged solution.
    - Privacy Threshold Assessment to identify if any Personally Identifiable Information (PII) is used with the leveraged solution. If PII is used a Privacy Impact Assessment will also be required.
    - Digital Identity Acceptance Statement identifying the Identity, Authentication, and Federation Assurance Levels required for the leveraged solution.
  - The CSP CRM is updated by labeling two columns (see below) to the right of the last column in the Customer Responsibility Matrix tab and completing those columns for all responsibilities listed.
    - Implementation Status (Yes/No)
    - Comments if No.
  - Any evidentiary artifacts supporting documents listed are stored in a central location for review.
  - Assessments for leveraged solutions will be performed as listed below. The assessment artifacts will be included as part of the authorization package.
    - FIPS 199 Low systems may use self-attestation as the assessment artifact.

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

- FIPS 199 Moderate systems must have an independent assessment[1] performed against the CRM controls/requirements using methods approved by the OCISO.

- **Approval Process**: A Leveraged XaaS Certification Memorandum is prepared documenting any less than fully implemented customer responsibilities. An ATO letter is prepared, which may be an update to an existing ATO letter for a system/platform. Templates are available on the InSite IT Security Forms and Aids page. A copy of the ATO Letter must be provided to the FedRAMP PMO. The ISSO and ISSM will coordinate delivery to FedRAMP.

  Note: For systems leveraging a FedRAMP XaaS solution, an ATO letter must be prepared for every instance of the leveraged solution.

5 GSA Standard A&A Process

All GSA A&A processes are based upon NIST SP 800-37. A depiction of the NIST RMF steps is provided in Figure 5-1.

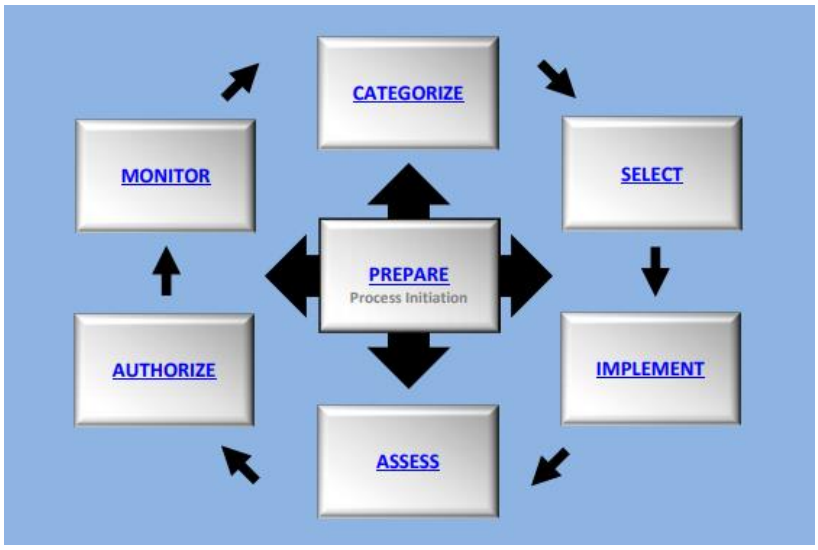

Figure 5-1. Risk Management Framework Steps (from NIST 800-37, Revision 2)

The RMF steps associated with the GSA Standard A&A Process are detailed in the following sections. Additional A&A processes GSA has developed or uses are identified in Section 4 which have been adapted or modified from the standard RMF processes. Documents required as part of a GSA A&A process are listed in Appendix C along with hyperlinks (where applicable) to resources containing document templates.

[1] Independence is defined as when assessors do not: (i) have a mutual or conflicting interest with the organizations where the assessments are being conducted; (ii) assess their own work; (iii) act as management or employees of the organizations they are assessing; or (iv) place themselves in positions of advocacy for the organizations acquiring their services.

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

The RMF steps in this section are documented in their sequential order from NIST SP 800-37. Similar to NIST SP 800-37, after the Prepare step the RMF steps may be completed in a non-sequential order due to the system type, the life cycle stage, and development process (e.g., agile development often generates multiple iterations of steps). When systems are in the Monitor step, changes to the system may cause multiple steps to be revisited. In addition, tasks in some steps may occur concurrently for efficiency. For example, in the Select step, the control selection, control tailoring, and some aspects of control allocation are interrelated which may benefit by considering them at the same time.

As required by EO 13800, GSA has aligned its risk management process with the CSF. The five core CSF Functions are:

- **Identify (ID):** Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.
- **Protect (PR):** Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
- **Detect (DE):** Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
- **Respond (RS):** Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.
- **Recover (RC):** Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

Appendix A contains a mapping of the NIST RMF steps and tasks to the five core functions of the CSF in Table A-1. Table A-2 provides the definitions for the CSF Categories and Subcategory Unique Identifiers.

5.1 RMF PREPARE Step

From NIST SP 800-37, "*The purpose of the **Prepare** step is to carry out essential activities at the organization, mission and business process, and information system levels of the organization to help prepare the organization to manage its security and privacy risks using the Risk Management Framework.*"

Organization Level Prepare Tasks

Additional details on the organizational prepare steps described in the following sections are included in CIO-IT Security-18-91: Risk Management Strategy (RMS), CIO-IT Security-18-90: Information Security Program Plan (ISPP), CIO-IT Security-12-66: Information Security Continuous Monitoring (ISCM) Strategy & Ongoing Authorization (OA) Program, CIO 2100.1, and guides describing GSA's various A&A processes identified in Section 4.

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

5.1.1 TASK P-1: Risk Management Roles

CIO 2100.1, Section 1.5 of this guide, and CIO-IT Security-18-91: Risk Management Strategy (RMS) identify and assign key roles for executing the RMF within GSA. The CISO, Authorizing Officials, ISSMs, ISSOs, System Owners, and subject matter experts from the OCISO and other GSA organizations facilitate the consistent application of cybersecurity risk management across GSA.

5.1.2 TASK P-2: Risk Management Strategy

The EMB, chaired by the Deputy Administrator who is also the SAORM manages enterprise risk at GSA. For cybersecurity risks, the ERES, co-led by the Deputy Performance Improvement Officer and the CISO, identifies and monitors agency-wide risks and ensures the EMB is updated on the risks and impacts to GSA. CIO-IT Security-18-91: Risk Management Strategy provides a comprehensive approach for framing, assessing, responding to, and monitoring risks associated with GSA information systems in accordance with Federal laws, regulations, and requirements. It addresses risk tolerance, determination, acceptance, mitigation, and communication within GSA and to external organizations. The GSA Privacy Program addresses privacy risks at GSA.

5.1.3 TASK P-3: Risk Assessment – Organization

The EMB along with the ERES address risks at the organizational level. The EMB meets periodically at the direction of the Deputy Administrator (Chair) or the Chief Financial Officer/Performance Improvement Officer (Deputy Chair) to assess and update organizational risks at GSA. CIO-IT Security-18-91: Risk Management Strategy contains additional details about the EMB and ERES.

5.1.4 TASK P-4: Organizationally – Tailored Control Baselines and Cybersecurity Framework Profiles (OPTIONAL)

The various GSA A&A processes listed in Section 4 of this guide, along with the GSA Control Tailoring Workbook, SSPP templates, and the controls listed in Section 9 of this guide, establish and identify GSA's tailored control baselines for systems.

5.1.5 TASK P-5: Common Control Identification

GSA IT Security-18-90, identifies enterprise-wide common and hybrid controls. It provides implementation details about common controls and common portions of hybrid controls for systems to inherit and information regarding system responsibilities for the hybrid controls.

The GSA is in the process of identifying the apportionment of controls for other common control sources such as GSA enterprise systems (e.g., general support systems, platforms) and other S/SO systems or sources. System Owners inheriting controls must ensure providing systems agree that they are providing the controls and then document this inheritance in their SSPPs. As the GSA moves SSPPs into Archer GRC control inheritance will be implemented such that common control providers will designate controls being provided and systems inheriting controls will identify controls they are inheriting and the systems they are inheriting them from.

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

As this information becomes available in Archer GRC some of the manual activities discussed will happen automatically.

Common control providers are responsible for:

- documenting common controls in an SSPP (or equivalent document prescribed by the organization);
- ensuring that common controls are developed, implemented, and assessed for effectiveness by qualified assessors with a level of independence required by the organization;
- documenting assessment findings in a security assessment report;
- producing a POA&M for all common controls deemed less than effective (i.e., having unacceptable weaknesses or deficiencies in the controls);
- receiving authorization for the common controls from the AO; and
- monitoring common control effectiveness on an ongoing basis.

The common control provider's SSPP, Security Assessment Report (SAR), and POA&M for common controls (or a summary of such information) should be made available to System Owners (whose systems are inheriting the controls) after the information is reviewed and approved by the AO responsible and accountable for the controls.

A Control Implementation Summary (CIS) table based on the system's control baseline must be completed. The table identifies control types (common, hybrid, system specific), implementation status (Fully Implemented, Partially Implemented, Planned, etc.), and responsibility (OCISO, GSS/Platform/System) for the system's controls. The table should be customized to the GSA S/SO or contractor's environment to account for additional designations of responsibility as necessary. CIS table templates are available for use on the IT Security Forms and Aids page.

The completed CIS table will be included as an attachment to the SSPP. It will be updated in subsequent steps of the RMF process, including after security control implementation and following security assessment to document the results of the review.

5.1.6 TASK P-6: Impact-Level Prioritization (Optional)

GSA has not performed this optional task at this time. Systems will continue to use their FIPS 199 security categorization of Low, Moderate, or High with no further priority or level within those categories. GSA has developed additional A&A processes, as listed in Section 4, which allows systems meeting the criteria for a specific process to streamline its A&A activities.

5.1.7 TASK P-7: Continuous Monitoring Strategy – Organization

The GSA continuous monitoring strategy leverages both manual and automated processes to monitor a system's security and privacy controls. The objective of the strategy is to ensure all key information security controls are periodically assessed for effectiveness. GSA's organizational continuous monitoring strategy leverages its deployment of Continuous

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

Diagnostics and Mitigation (CDM) and other Enterprise Security Management tools (e.g., Netsparker, Enterprise Logging Platform) to monitor the security of GSA's systems. CIO-IT Security-12-66: Information Security Continuous Monitoring (ISCM) Strategy & Ongoing Authorization (OA) Program provides more details on how GSA continuously monitors vulnerabilities, threats, and actions taken to reduce, mitigate, or eliminate them. Key components of GSA's strategy are regular vulnerability scanning activities and security configuration checks, the requirement to maintain A&A documents in an "as-is" state, management and review of POA&Ms, and ISSO Checklists within Archer GRC.

System Level Prepare Tasks

Additional details on the System-Level prepare tasks described in the following sections are included in CIO-IT Security-21-114: Clean Authorization to Operate (ATO)—this guide is under development and will be posted to the InSite IT Security Procedural Guides web page when complete. It provides a clearly defined, phased approach for successfully completing the A&A of a system in order for the system to receive an ATO. The Clean ATO guide includes links to a number of standard operating procedures (SOPs) that provide additional details regarding executing tasks that occur prior to assessments (Prepare, Select, Implement), during assessments (Assess), and after assessments (Authorize) to ensure systems can effectively and efficiently receive an ATO.

5.1.8 TASK P-8: Mission or Business Focus

The information system's missions, business functions, processes, and purposes the system is intended to support is to be documented in Section 9, General Description, of the GSA SSPP template. The system owner in collaboration with the ISSO completes this section of the SSPP.

5.1.9 TASK P-9: System Stakeholders

The information system's system owner, AO, ISSO, ISSM, and other stakeholders (e.g., custodian, CSP, etc.) is to be documented in Sections 3-6 of the GSA SSPP template. The system owner in collaboration with the ISSO completes this section of the SSPP.

5.1.10 TASK P-10: Asset Identification

The information system's assets, both tangible and intangible, are to be documented in Sections 8-10 of the GSA SSPP template. Tangible elements include physical elements, human elements, and technological elements. Intangible elements include data/information, firmware, software, services, and processes/functions. For example, the assets would include the locations, types of information, hardware and software components, and users. The system owner in collaboration with the ISSO completes this section of the SSPP.

5.1.11 TASK P-11: Authorization Boundary

The information system's authorization boundary is documented in Sections 9-11 of the GSA SSPP template. The system owner in collaboration with the AO and ISSO completes this section of the SSPP. The authorization boundary includes the system components, network

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

architecture, and inventory. Diagrams showing connections and interconnections must clearly depict the authorization boundary. The tables for interconnections in the SSPP must be completed, including agreements concerning those interconnections, as applicable. Per GSA IT Security Policy 2100.1, "All interconnections between GSA and external entities including off-site contractors or Federal agency/departments must be documented in ISA that is approved by the AOs and concurred by the GSA CISO". Per NIST 800-47, "Security Guide for Interconnecting Information Technology Systems" an interconnection is the direct connection of two or more IT systems for the purpose of sharing data and other information resources through a pipe, such as ISDN, T1, T3, DS3, VPN, API, etc.

5.1.12 TASK P-12: Information Types

The information system's information types are documented in Section 2 of the GSA SSPP template. The data owner(s) and system owner in collaboration with the ISSO completes this section of the SSPP. A GSA FIPS 199 Security Categorization document must be completed and attached to the SSPP. It will identify the information system types and overall security categorization of the system based on the information types listed in NIST SP 800-60 Volumes I and II.

5.1.13 TASK P-13: Information Life Cycle

The life cycle of information must be described to include its creation or collection, processing, transmission, use, storage, and disposition. Sections 10.4 and 10.5 of the GSA SSPP template must be completed to understand much of the information life cycle. Those sections describe how data flows within and into and out of the system. Other sections of the SSPP, such as the Section 9 where the system missions, functions, and business processes must describe the collection or creation of information in order to fulfill the overall mission of the system. Specific controls regarding encryption of data and media protection and sanitization provide additional details on the transmission and disposition of information.

5.1.14 TASK P-14: Risk Assessment – System

An initial security assessment must be performed prior to a system receiving an ATO. This assessment includes assessing the risk of operating the system as detailed in the RMF Assess Step in Section 5.5 of this guide. Assessment of risk is also performed as part of the RMF Monitor Step in Section 5.7 of this guide.

5.1.15 TASK P-15: Requirements Definition

Completion of the GSA FIPS 199 Security Categorization and Privacy Threshold Assessment/Privacy Impact Assessment assessments provide the FIPS 199 security category of the system and the determination on whether the system contains Personally Identifiable Information (PII). These two documents determine the initial set of security requirements/controls that the system must meet/implement. GSA's various A&A processes, the Control Tailoring Workbook, SSPP templates, and Section 9 of this guide further define the exact set of requirements for the system and the controls it must implement.

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

5.1.16 TASK P-16: Enterprise Architecture

GSA's Office of Enterprise Planning and Governance (IDR) in GSA IT is responsible for GSA's enterprise architecture. GSA Order CIO 2110.4, "GSA Enterprise Architecture Policy" utilizes GSA's strategic goals, mission and support services, data, and enabling technologies to communicate the business vision and target architecture in conjunction with the GSA Performance Management, Capital Planning and Investment Control (CPIC), and Solutions Life Cycle (SLC) processes. The Security Engineering Division (ISE) in OCISO works closely with IDR and other Services/Staff Offices to facilitate integration of security standards/requirements into development efforts, ensuring secure outcomes as a matter of routine. Additional information is available in CIO-IT Security-18-90: Information Security Program Plan and the GSA EA Analytics & Reporting (GEAR) website.

5.1.17 TASK P-17: Requirements Allocation

Controls are allocated based on the common, hybrid, and system specific designations identified in CIO-IT Security-18-90: Information Security Program Plan, GSA's various A&A processes, the Control Tailoring Workbook, and SSPP templates. GSA is also in the process of a control allocation mapping among its GSSs and Platforms to identify controls common or hybrid at those levels that systems can inherit. Allocation of controls to system components is the purview of the system owner in collaboration with the OCISO.

5.1.18 TASK P-18: System Registration

Program Managers and Project Managers collaborate with the GSA S/SOs as new systems are being considered for design, development, piloting, or implementation. GSA's ISSMs and ISSOs work closely with those offices and personnel to ensure systems are registered into the GSA system inventory as early as possible. Archer GRC is the repository for GSA's system inventory. Systems are registered in it as soon as they are identified and categorized as pending. They will stay in this status until they are placed into production.

5.2 RMF CATEGORIZE Step

From NIST SP 800-37, "*The purpose of the **Categorize** step is to inform organizational risk management processes and tasks by determining the adverse impact to organizational operations and assets, individuals, other organizations, and the Nation with respect to the loss of confidentiality, integrity, and availability of organizational systems and the information processed, stored, and transmitted by those systems.*"

The following tasks detail the actions in the RMF categorize step. Additional details may be found in CIO-IT Security-21-114: Clean Authorization to Operate (ATO)—this guide is under development. As GSA implements automation into its A&A processes, the tasks described in the following sections will be migrated, as much as possible, to GSA's implementation of Archer GRC.

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

5.2.1 TASK C-1: System Description

The information system is described throughout Sections 1-12 of the GSA SSPP template. The system owner in collaboration with the ISSO completes these sections of the SSPP. These sections cover the system's operational environment, hardware, and software inventory, FIPS 199 security categorization, data, users, roles, architecture, connections, etc. Each section should be sufficiently detailed to permit readers to understand the business functions of the system, how the system architecture and components support those functions, how data is collected, processed, and transmitted internally and externally (i.e., data flow), the sensitivity of the data the system handles, the user base, and the key points of contact. The system owner in collaboration with the ISSO completes these sections of the SSPP.

5.2.2 TASK C-2: System Categorization

Use GSA's FIPS 199 Security Categorization Template to identify the information types handled by the system. Once completed it is summarized in Section of the SSPP with the completed FIPS 199 template attached to the SSPP. NIST SP 800-60 Volumes I and II are used to identify the information types handled by the system. The result of the system categorization is used in a future step to select security controls for the system. The data owner collaborates with the system owner and the ISSO to complete the template.

5.2.3 TASK C-3: System Categorization Review and Approval

The system FIPS 199 security categorization from the previous step must be reviewed and approved by the AO and CISO or their designated representatives. The CPO, or designated representative, must approve the security categorization for systems with PII. Delegated representatives must be Federal employees. The ISSO collaborates with the AO, OCISO, Privacy Team, and data owner as necessary to have the FIPS 199 security categorization approved.

5.3 RMF SELECT Step

From NIST SP 800-37, "*The purpose of the **Select** step is to select, tailor, and document the controls necessary to protect the information system and organization commensurate with risk to organizational operations and assets, individuals, other organizations, and the Nation.*"

The following tasks detail the actions in the RMF select step. Additional details may be found in CIO-IT Security-21-114: Clean Authorization to Operate (ATO) Process)—this guide is under development. As GSA implements automation into its A&A processes, the tasks described in the following sections will be migrated, as much as possible, to GSA's implementation of Archer GRC.

5.3.1 TASK S-1: Control Selection

The system's FIPS 199 security categorization and PTA/PIAs determine the initial set of security controls that the system must meet/implement. GSA's various A&A processes, the CTW, and Section 9 of this guide further define the specific set of controls the system must implement.

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

The System Owner collaborates with the AO, ISSM, ISSO, and Privacy Team as necessary to complete the control selection task.

Note: Additional Federal requirements such as DHS Cybersecurity Directives must be included in a system's set of requirements.

5.3.2 TASK S-2: Control Tailoring

After the security controls for a system have been selected in the previous task, tailoring of those controls commences. Tailoring includes:

- Determining common controls the system inherits;
- Assigning values to any parameters identified as being left up to the system for assignment and requiring GSA AO and CISO approval;
- Determining if any compensating or supplemental controls are required to address unique organizational and/or system specific needs. These needs may be based on a risk assessment (either formal or informal), local conditions including environment of operation, organization-specific security requirements, specific threat information, cost-benefit analyses, or special circumstances.

Justification or rationale for tailoring actions is required, especially where the CISO and AO must approve assignments and if any controls are identified as not applicable to the system or its environment.

Systems must complete a CTW and provide it as an attachment to the SSPP. The CTW identifies the GSA defined values for NIST SP 800-53 control assignments and selections. The selected security controls including any controls or enhancements selected above the baseline for the information system will be documented in the SSPP. Both the SSPP and the CTW identify parameter assignments or selections deferred to the S/SO or contractor for recommendation and approval by the GSA AO and CISO. The CTW contains columns for identifying the defined values and GSA approval of the values.

Similarly, systems must complete a CIS which identifies the control types (common, hybrid, system specific), implementation status (Fully Implemented, Partially Implemented, Planned, etc.), and responsibility (OCISO, GSS/Platform/System) for the system's controls. It will be updated in subsequent steps of the RMF process, including after security control implementation and following security assessment to document the results of the review.

The System Owner collaborates with the ISSM, ISSO, Privacy Team as necessary, and other System Owners (regarding common/hybrid controls) to complete control tailoring.

5.3.3 TASK S-3: Control Allocation

As part of Tasks P-5: Common Control Identification and P-17: Requirements Allocation the GSA OCISO and the system owner in collaboration with the OCSIO identified and allocated controls to the system. These controls were further defined in the previous two tasks. Now the system

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

owner collaborates with the ISSO to identify how controls have been allocated. This task includes verifying the common, hybrid, and system specific designations of controls and the components or elements within the system to which controls are allocated. For example, boundary protection controls may be allocated to components that manage and monitor the system boundary, access control to components that manage access to the system by users and other systems or between components of the systems. The details of control allocation must be documented in the SSPP. The System Owner collaborates with the ISSM, ISSO, Privacy Team as necessary, and other System Owners (regarding common/hybrid controls) to complete control allocation.

5.3.4 TASK S-4: Documentation of Planned Control Implementations

Systems must complete an SSPP using the GSA SSPP Template, including the appendices and attachments, as applicable, identified in Appendix C. The SSPP provides an overview of the security requirements for the information system and, in this step, describes the controls planned for implementation to provide a level of security appropriate for the information to be transmitted, processed, or stored by the system. Inherited controls should be included. Detailed instructions for completing the SSPP are in the GSA SSPP Template on the InSite IT Security Forms and Aids web page; a brief summary of those instructions regarding controls is:

- Each control part must be addressed (e.g., Part a, Part b, etc.);
- Do not just reiterate the control statement. Describe the "who, what, when, where, and how" controls are implemented;
- Address the entire IT stack (e.g., OS, database, network, etc.) and all processes that implement a control;
- Describe how GSA-defined parameters are met;
- Ensure parameters deferred to S/SO or Contractor recommendation and AO and CISO approval are defined and it is described how those parameters are met;
- If controls are planned versus implemented, a time bound plan must be a part of the implementation details;
- If controls are identified as not applicable, a justification and supporting evidentiary artifacts must be presented.

The System Owner collaborates with the ISSO, Privacy Team as necessary, other System Owners (regarding common/hybrid controls), and others to complete the SSPP planned control implementations.

5.3.5 TASK S-5: Continuous Monitoring Strategy – System

Systems must develop a system-level strategy for monitoring its security controls. The system level strategy must be aligned with RMF Step Monitor and CIO-IT Security-12-66: Information Security Continuous Monitoring (ISCM) Strategy & Ongoing Authorization (OA) Program and CIO-IT Security-21-114: Management Implementation Plan)—this guide is under development. The strategy is to address monitoring of controls that are not monitored as part of GSA's ISCM strategy and the frequency of monitoring. It defines how system changes are monitored, how

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

risk assessed, and reporting on monitoring and the reporting of results. The System Owner collaborates with the ISSM, ISSO, Privacy Team as necessary, and others to establish the system-level continuous monitoring strategy.

5.3.6 TASK S-6: Plan Review and Approval

The SSPP must be reviewed and approved. The System Owner collaborates with the ISSM, ISSO, Data Owners, Privacy Team as necessary, and other System Owners (regarding common/hybrid controls), and others to complete the SSPP, including appendices and attachments.

For new systems under development, note that in the Select Step, implementation details may not be fully described since the exact implementation to satisfy control requirements may not be complete. When the SSPP has been completed by the System Owner, ISSO (and Vendor ISSO if applicable), and the ISSM it is signed by each of them. The SSPP and appendices/attachments as listed in Appendix C will be updated and completed as the security controls are implemented in RMF Implement Step.

Note: Approving the security plan via the signatures noted is an agreement that the set of security controls (system-specific, hybrid, and/or common controls) proposed to meet the security requirements for the information system are sufficient. This approval allows the next step in the RMF to commence (i.e., the implementation of the security controls).

The Security Engineering Division (ISE) in the OCISO must review and approve the Security Architecture before the system's security controls are implemented. Additional details on developing and having the SSPP approved are contained in CIO-IT Security-21-114: Clean Authorization to Operate (ATO)—this guide is under development. RMF Implement Step

5.4 RMF IMPLEMENT Step

From NIST SP 800-37, "*The purpose of the **Implement** step is to implement the controls in the security and privacy plans for the system and for the organization and to document in a baseline configuration, the specific details of the control implementation.*"

The following tasks detail the actions in the RMF Implement step. Additional details may be found in CIO-IT Security-21-114: Clean Authorization to Operate (ATO)—this guide is under development. As GSA implements automation into its A&A processes, the tasks described in the following sections will be migrated, as much as possible, to GSA's implementation of Archer GRC.

5.4.1 TASK I-1: Control Implementation

Describe the security and privacy control implementation in the SSPP; providing a functional description of how the control is satisfied. Security control implementation should be consistent with the GSA enterprise architecture and information security architecture. IT systems shall be configured and hardened using GSA IT security hardening guidelines (i.e.,

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

security benchmarks), NIST guidelines, Center for Internet Security guidelines, or industry best practice guidelines, as deemed appropriate by the AO.

To the greatest extent possible, systems are encouraged to conduct initial security control assessments (also referred to as developmental testing and evaluation) during information system development and implementation. Such testing conducted in parallel with the development and implementation of the system facilitates the early identification of weaknesses and deficiencies and provides the most cost-effective method for initiating corrective actions.

Systems leveraging a cloud solution must implement the customer responsibilities identified in the CSP's CRM. Only customer responsibilities associated with NIST controls in the system's FIPS 199 control baselines must be addressed. For example, if a system is FIPS 199 Low and the CSP CRM includes FIPS 199 Moderate controls only the FIPS 199 Low controls will be addressed (and GSA OCISO specified controls, as necessary).

Federal requirements such as DHS Cybersecurity Directives include specific implementation instructions which must be fulfilled to secure the system and comply with the requirements.

The security control implementation descriptions should include planned inputs, expected behavior, and expected outputs (where appropriate) that are typical for technical controls. The SSPP should also address platform dependencies and include any additional information necessary to describe how the security capability required by the security control is achieved at the level of detail sufficient to support control assessment in RMF Step 4.

Security controls are documented in Section 13 of the SSPP. This section must provide a thorough description of how the NIST SP 800-53 security controls for the system are being implemented or planned to be implemented. Detailed instructions for completing the SSPP are in the GSA SSPP Template, on the InSite IT Security Forms and Aids web page. For each control, descriptions must include:

- Describing how (including, what, when, where, and who) the security control is being implemented or planned to be implemented for all parts of the control;
- Identifying any scoping guidance that has been applied, including the type and;
- Explaining how all specified parameters have been met (i.e., not just stating they have been met-describe the how);
- Establishing time bound plans are described for planned controls;
- Ensuring controls identified as Not Applicable a rationale and supporting evidentiary artifacts must be provided.
- Systems with multiple components or subsystems must describe control implementations across all components.
- Systems leveraging a cloud solution must describe how the customer responsibilities in the CSP's CRM are implemented.

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

Systems leveraging a cloud solution must implement the customer responsibilities identified in the CSP's CRM. Only customer responsibilities associated with NIST controls in the system's FIPS 199 control baselines must be addressed. For example, if a system is FIPS 199 Low and the CSP CRM includes FIPS 199 Moderate controls only the FIPS 199 Low controls will be addressed (and GSA OCISO specified controls, as necessary).

The System Owner collaborates with the ISSM, ISSO, Privacy Team as necessary, other System Owners (regarding common/hybrid controls), and others to complete all control implementations in the SSPP.

5.4.2 TASK I-2: Update Control Implementation

During development or in the course of operating and maintaining the system the implementation details of controls may change. Changes occur for many reasons, including by not limited to infeasibility of the design, new capabilities being made available, patches and upgrades to the system. The SSPP must be updated to reflect any changed implementation details so the SSPP always reflects the "as implemented" state of the system. In this manner when assessments, the next RMF step, occurs the assessors can determine if the system reflects its documented state or there are inconsistencies that need to be rectified.

The System Owner collaborates with the ISSM, ISSO, Privacy Team as necessary, other System Owners (regarding common/hybrid controls), and others to update control implementations in the SSPP as necessary.

5.5 RMF ASSESS Step

From NIST SP 800-37, "*The purpose of the **Assess** step is to determine if the controls selected for implementation are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security and privacy requirements for the system and the organization.*"

The following tasks detail the actions in the RMF Assess Step. Additional details may be found in CIO-IT Security-21-114: Clean Authorization to Operate (ATO)—this guide is under development. As GSA implements automation into its A&A processes, the tasks described in the following sections will be migrated, as much as possible, to GSA's implementation of Archer GRC.

5.5.1 TASK A-1: Assessor Selection

The key to effective assessments is having assessors with the required skills, abilities, and technical knowledge to develop assessment plans, assess controls, and prepare assessment reports. The level of independence of assessors required at GSA is (as noted regarding NIST SP 800-53 control CA-2, Enhancement 1:

> Independence is defined as when assessors do not: (i) have a mutual or conflicting interest with the organizations where the assessments are being

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

conducted; (ii) assess their own work; (iii) act as management or employees of the organizations they are assessing; or (iv) place themselves in positions of advocacy for the organizations acquiring their services.

The GSA Lead Assessor selects the assessors for a system. Additional details on selecting assessors may be found in CIO-IT Security-21-114: Clean Authorization to Operate (ATO)—this guide is under development.

5.5.2 TASK A-2: Assessment Plan

Assessors must develop and obtain approval of a Security Assessment Plan (SAP) which will be leveraged to assess the security controls of the information system. The SAP will provide system background information, the objectives for the security control assessment, the assessment approach, and the assessment test cases to be used in Task A-3. Developing the plan may require updates and/or supplements to GSA's NIST 800-53 Revision 5 Test Cases. As necessary assessors will incorporate additional assessment test cases for any supplemented controls and/or control enhancements added during RMF Select step.

Note: Assessment of additional Federal requirements including, but not limited to, DHS Cybersecurity Directives (i.e., BODs/EDs) must be included in the SAP as appropriate.

The following security assessment requirements must be defined in the SAP and implemented for all information systems per its FIPS 199 impact level:

- **FIPS 199 Moderate** and **High** impact systems must be assessed by an independent third party. The use of an independent assessment team reduces the potential for impartiality or conflicts of interest, when verifying the implementation status and effectiveness of the security controls. Independence, per NIST, is impartiality where the assessors are free from any perceived or actual conflicts of interest with respect to the development, operation, and/or management of the information system or the determination of security control effectiveness.
- **All FIPS 199 impact level** information systems must conduct authenticated vulnerability scanning of their servers' operating systems as part of security assessment activities. Configuration/compliance scans shall be to GSA technical guidelines, NIST guidelines, Center for Internet Security guidelines, or industry best practice guidelines, as deemed appropriate and approved by the AO and CISO. Where a GSA benchmark exists, configuration scanning must be to the GSA benchmarks. Any scanning tool configured to support the benchmarks or guidelines identified may be used. Contact OCISO for information on the current tools in use or if there is a question about a specific tool.
- **All FIPS 199 impact level** information systems with web servers must conduct an authenticated vulnerability scan for the most current Open Web Application Security Project (OWASP) Top Ten Web Application Security Risks. Any scanning tool configured to support the OWASP Top 10 may be used. Contact OCISO for information on the current tools in use or if there is a question about a specific tool. If necessary, manual

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

testing and/or verification using the most current OWASP Testing Guide and/or CIO-IT Security-07-35: Web Application Security is also acceptable.

- **All FIPS 199 impact level** information systems with database servers will have their databases scanned as part of their OS vulnerability scanning.
- **All Internet accessible systems, FIPS 199 High impact level, and High Value Asset (HVA) information** systems, are required to complete an independent penetration test (or 'pentest') and provide a Penetration Test Report documenting the results of the exercise as part of the A&A package. These tests will be conducted in accordance with CIO-IT Security-11-51: Conducting Penetration Test Exercises.
- **All FIPS 199 impact level** information systems are encouraged (and required per the Lightweight and MiSaaS authorization processes) by GSA OCISO to conduct a code analysis using tools to examine the software for common flaws and document the results in a Code Review Report per NIST SP 800-53 Control SA-11 enhancement (1).

The SAP must be reviewed and approved by the ISSO and ISSM to ensure the plan:

- includes all appropriate security controls;
- is consistent with system/organizational security objectives;
- employs required assessment tools and techniques;
- provides assessment test cases; and
- defines the scope of the assessment and any conditions or restrictions.

The overall purpose of the SAP approval is two-fold: (1) to establish the appropriate expectations for the security control assessment; and (2) to bound the level of effort for the security control assessment.

5.5.3 TASK A-3: Control Assessments

Assessors assess the security controls following the SAP and using the NIST 800-53, Revision 5 Test Cases, including any supplemental or updated tests based on the specific system as identified in Task A-2 (e.g., assessing BODs or other Federal requirements). The assessment determines if the controls implemented in the RMF Implement Step are operating as intended and producing the desired outcome with respect to meeting the security requirements for the information system. Systems leveraging cloud solutions must include assessing the implementation of customer responsibilities from a CSP's CRM in the assessment.

5.5.4 TASK A-4: Assessment Reports

Assessors prepare a Security Assessment Report (SAR) documenting the issues, findings, and recommendations of the security control assessment (including, if applicable, a penetration test report as an attachment). The SAR documents the assessment findings with recommendation(s) and risk determinations based on NIST SP 800-30, Revision 1, *"Guide for Conducting Risk Assessments."* Multiple findings regarding the SSPP (Control PL-2) can be consolidated into one finding and associated with PL-2. All other findings (including scan findings) rated Low or above are reported individually in the SAR.

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

Additional information on addressing findings based on the source of findings (e.g., test cases, scans, pen tests) is provided in the SAR template available on InSite. The SAR will be included as part of the authorization package.

The risk assessment should consist of the following steps:

- Identify the list of threats and threat sources to the system. The list should include but not be limited to adversarial outsider and insider threats, accidental user threats, structural threats to its components and facilities, environmental threats to the systems facilities and supporting services.
- Align threat sources, impacts, and events with vulnerabilities.
- Assess each not fully met security control and vulnerability identified during the security assessment. Evaluating the likelihood that threat sources and events will exploit each identified vulnerability.
- Assess the possible impact to the system and GSA if the vulnerability was exploited.
- Make a determination of risk based on the likelihood the threat will exploit the vulnerability, and the resulting impact.
- Evaluate the risks of all identified vulnerabilities to determine an overall level of risk for the system or application.

Assessments must include vulnerability description, assessed risk, and recommendations for correcting the vulnerability. Assessment results for subsystems, if any, should be referenced, as appropriate, in the SAR.

Review and consider ALL risk categories in the process of preparing the final SAR. It is a common mistake to ignore some classes of vulnerabilities or findings since they are incorrectly believed to be "low risk." However, scanning tools generally categorize findings without context. They may identify false positive findings that are not real issues and false negative findings or "low/info risk" findings that may be real issues. A human reader with context and an understanding of how the system works and its environment will understand that some findings are more important than initially labeled. Moreover, low risk items often enhance the risk of other issues or can successfully be combined to generate higher risk. Once identified, they should be rated appropriately (i.e., no longer Low) in the final SAR. FIPS 199 Low or Moderate systems can possess Very High (Critical)/High risk findings the same as FIPS 199 High systems.

5.5.5 TASK A-5: Remediation Actions

Systems may perform initial remediation actions on security controls based on the findings and recommendations of the SAR and have the assessors reassess remediated control(s), as appropriate. Assessors should identify remediated vulnerabilities as “Remediated” in the final SAR. Similarly, any findings proven to be a false positive should be identified as “False Positive.” Additional instructions are provided in the SAR template on the InSite Forms and Aids page. The assessors in coordination with the System Owner, ISSO, and other system personnel validate remediated and false positive findings.

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

5.5.6 TASK A-6: Plan of Action and Milestones

The ISSO collaborates with the System Owner, other system personnel, and the ISSM and prepares POA&Ms as follows:

5.5.6.1 POA&Ms from a SAR

POA&Ms from a SAR adhere to the following conventions:

- Do not create POA&Ms for any vulnerabilities identified as ‘‘Remediated” or “False Positive” in the SAR.
- Create POA&Ms for all other vulnerabilities (including scan findings) in the SAR as individual POA&Ms.

5.5.6.2 POA&Ms from Other Assessments

POA&Ms from other assessments adhere to the following conventions:

- All findings from audits become individual POA&Ms.
- All findings indicating End-of-Life (EOL) software or components become individual POA&Ms.
- Vulnerability Scans
  - If vulnerabilities in the Cybersecurity & Infrastructure Security Agency (CISA) Known Exploited Vulnerabilities (KEV) Catalog cannot be readily corrected within the KEV timeline an additional 14-day grace period will be given. After this period, the CIO and AO will have the option of approving the creation of a POA&M for no longer than 60 days beyond the KEV’s remediation date.
  - POA&Ms must be created for vulnerabilities exceeding the remediation timelines listed below.
    - 15 days for Critical (Very High) vulnerabilities for Internet-accessible systems or services.
    - 30 days for Critical (Very High) and High vulnerabilities.
    - 90 days for Moderate vulnerabilities.
    - 120 days for Low vulnerabilities for Internet-accessible systems/services.
  - External Vendor/Contractor systems – Low vulnerabilities must have POA&Ms established within 90 days, although there is no remediation deadline (other than as listed above).
- Configuration/Compliance Scans. A FISMA system must monitor compliance to all the configuration settings required by GSA hardening guides. Each configuration setting must be covered by one of the following clauses:
  - The configuration setting is compliant - The asset’s setting is either
    - Equal to the setting required, or
    - More restrictive than the setting required.
  - The configuration setting is not compliant - The asset is configured with a more liberal setting than required. In this case, the non-compliant configuration setting needs to be accounted for in one of the following ways:

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

- Deviation - The non-compliant setting is covered by an approved deviation.
- POA&M - If the composite compliance percentage of all assets with a single operating system is below 85% for over 90 days, a POA&M must be created for the non-compliant operating system. The resultant POA&M will state:

  "Configuration/compliance scans indicate that [ENTER OPERATING SYSTEM] has been below 85% compliant for over 90 days."

Note: GSA systems not being scanned under GSA's vulnerability scanning program must provide supporting scan reports to the OCISO ISP Division as part of updating the POA&M via the POA&M Google Shared Drives. Scan folders are located inside of appropriate system Shared Drives for ISSOs to upload vendor provided scans.

The POA&M describes how the System Owner intends to address vulnerabilities (i.e., reduce, eliminate, or mitigate vulnerabilities). A POA&M Template and details on developing POA&Ms are contained in the POA&M procedural guide and on the POA&M Guidance Google Shared Drive. A GSA POA&M Template may be obtained by contacting ispcompliance@gsa.gov.

Update the SSPP to reflect the results of the security assessment and any modifications to the security controls in the information system. This is necessary to account for any modifications made to address recommendations for corrective actions from the security assessor. Following completion of security assessment activities, the SSPP should reflect the actual state of the security controls implemented in the system. Update the GSA CTW and applicable Control Implementation Summary Table. The updated documents must be included as appendices to the SSPP.

Note: GSA tracks all POA&Ms on POA&M Shared Drives which serve as the primary tool for the management, storage, and dissemination of GSA system and program POA&Ms.

5.6 RMF AUTHORIZE Step

From NIST SP 800-37, "*The purpose of the **Authorize** step is to provide organizational accountability by requiring a senior management official to determine if the security and privacy risk (including supply chain risk) to organizational operations and assets, individuals, other organizations, or the Nation based on the operation of a system or the use of common controls, is acceptable.*"

The following tasks detail the actions in the RMF Authorize Step. Additional details may be found in CIO-IT Security-21-114: Clean Authorization to Operate (ATO)—this guide is under development. As GSA implements automation into its A&A processes, the tasks described in the following sections will be migrated, as much as possible, to GSA's implementation of Archer GRC.

5.6.1 TASK R-1: Authorization Package

The ISSO assembles the security authorization package. For GSA's Standard A&A process, the security authorization package includes:

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

- SSPP (with all appendices and attachments);
- Security Assessment Report (with all appendices and attachments);
- POA&M;
- Certification Memorandum;
- ATO Letter.

Note: The documents outlined for the Security Authorization Package (above) are required for the GSA Standard A&A Process. The documentation required and links to document templates for other A&A processes GSA uses (and the standard process) are listed in Appendix C.

5.6.2 TASK R-2: Risk Analysis and Determination

The AO makes the risk level determination. To do so, the AO assesses all the information documented in the Security Authorization Package regarding the current security state of the system or the common controls inherited by the system and the recommendations for addressing any residual risks. The AO consults with the CISO, System Owner, ISSM, ISSO, and others as necessary to determine if the package provides enough information to establish a credible level of risk.

5.6.3 TASK R-3: Risk Response

The AO in consultation with the CISO, System Owner, ISSM, ISSO, and others as necessary determines if the residual risks in operating the system need to be mitigated or can be accepted and managed via POA&Ms prior to authorization. As part of risk response prioritization of risks POA&Ms can be prioritized to focus resources on the POA&Ms that will have the greatest impact in reducing risk.

5.6.4 TASK R-4: Authorization Decision

The explicit acceptance of risk is the responsibility of the AO. The AO determines if the risk to organizational operations, organizational assets, individuals, other organizations, or the Nation is acceptable. The AO must consider many factors, balancing security considerations with mission and operational needs. The AO issues an authorization decision for the information system and the common controls inherited by the system after reviewing all of the relevant information. The AO must determine if the remaining known vulnerabilities in the information system pose an acceptable level of risk to agency operations, assets, and individuals and determine if the risk to the agency is acceptable.

The preparation and routing for review and signature of the system's authorization package is detailed in CIO-IT Security-21-114)—this guide is under development—and is summarized as follows:

- IST quality checks and validates the package and prepares a Certification Memorandum and uploads documents to Archer GRC (if not already uploaded).
- ISP reviews Archer GRC to ensure the entire package is present, then reviews the package for completeness and consistency.

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

- ISP coordinates with the ISSM on the preparation of the ATO Letter and uploads it to Docusign.
- The CISO reviews the package and coordinates with the ISSM and others and signs the letter (or directs changes).
- The AO is briefed and based on the evidence provided and whether it establishes an acceptable risk decides to:
  - Authorize system operation without any restrictions or limitations on its operations.
  - Authorize system operation with restrictions/limitations on its operations. The POA&M must include detailed corrective actions to correct the deficiencies requiring the restrictions/limitations. The ISSM/ISSO must resubmit an updated authorization package upon completion of required POA&M actions to move to a full ATO without any restrictions/limitations.
  - Not authorize the system for operation.

5.6.5 TASK R-5: Authorization Reporting

Authorization decisions are reflected in the system information in Archer GRC with high-level A&A metric data published organization-wide on the (GEAR) website. Any risks that need to be raised to the enterprise level are reported through the ERES and EMB. The CISO is co-chair of the ERES with members from GSA S/SO/Rs to ensure appropriate risks are raised that may influence GSA's strategy, budget planning, and resource allocation decisions.

5.7 RMF MONITOR Step

From NIST SP 800-37, "The purpose of the **Monitor** step is to maintain an ongoing situational awareness about the security and privacy posture of the information system and the organization in support of risk management decisions."

The following tasks detail the actions in the RMF Monitor Step**Error! Not a valid bookmark self-reference.**. As GSA implements automation into its A&A processes, the tasks described in the following sections will be migrated, as much as possible, to GSA's implementation of Archer GRC.

5.7.1 TASK M-1: System and Environment Changes

System Owners must determine the security impact of proposed or actual changes to the information system and its operational environment. Per CIO-IT Security-01-05, proposed system changes must be evaluated to determine potential security impacts. An impact analysis of each proposed change will be conducted using the following as a guideline:

- Whether the change is viable and improves the performance or the security of the system;
- Whether the change is technically correct, necessary, and feasible within the system constraints;
- Whether system security will be affected by the change;
- Whether associated costs for implementing the change were considered; and

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

- Whether security components are affected by the change.

As outlined within CIO-IT Security-18-91 GSA has a rigorous configuration change management process. The RMS states:

- IT changes are to be requested through a defined CM approval process (e.g., a chartered Configuration Control Board [CCB]) that documents the nature of the change, the criticality, impacts on the user community, testing and rollback procedures, stakeholders, and points of contact.
- System changes are to be tested and validated prior to implementation into the production environment.
- Configuration settings and configuration baselines are to be updated as necessary to meet new technical and/or security requirements and are controlled through the CM process.

Changes may be required by outside influences. For example, if a successful exploit or identified vulnerability can be resolved or mitigated by configuration or process changes, the same CM process described above must be followed to ensure the resolution does not have unintended consequences.

5.7.2 TASK M-2: Ongoing Assessments

System Owners are responsible for assessing a subset of the NIST SP 800-53 security controls employed within and inherited by the information system in accordance with GSA's monitoring strategy. Per CIO-IT 01-05, the implemented CM process calls for continuous system monitoring to ensure that systems are operating as intended and that implemented changes do not adversely impact either the performance or security posture of the systems. Per CIO-IT Security-04-26, GSA's annual FISMA self-assessments will assess a subset of security controls. Controls are selected based on an analysis of past audit findings, known weaknesses or controls that have resulted in security breaches, key controls (e.g., Showstopper controls, critical controls), and volatile controls that should be assessed frequently. Ongoing assessments include penetration tests and OIG audits that are performed on systems.

GSA conducts ongoing assessments by leveraging its deployment of Continuous Diagnostics and Mitigation (CDM) and other Enterprise Security Management tools. GSA's tool stack facilitates the ongoing assessments of GSA information systems by performing vulnerability scans and checking the configuration settings of systems against GSA required hardening or benchmarks.

5.7.3 TASK M-3: Ongoing Risk Response

ISSOs, System Owners, and system, network, and database administrators, will coordinate and perform remediation actions based upon the results of ongoing monitoring activities, assessment of risk, and outstanding items in the system's POA&M. CIO-IT Security-01-05 outlines the implementation of a CM process designed to lower the potential risk to a network by requiring regular "patching" or repairing of known vulnerabilities. CIO-IT Security-01-05 addresses the required steps for implementing changes; Identifying Changes, Evaluating Change

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

Requests, Decision Implementation, and Implementing Approved Change Requests. Per CIO-IT Security-18-91, risk mitigation shall be the appropriate risk response for all critical/very high and high risks vulnerabilities that can be exploited from the Internet and cannot be accepted, avoided, shared, or transferred. Risks from identified vulnerabilities must be remediated based on the timelines specified in NIST SP 800-53 control RA-5 in Section 8.3.4. No standard remediation timeline is established for Low/Very Low vulnerabilities identified for non-Internet accessible systems/services; they are to be addressed on a case-by-case basis. Risk mitigation strategies may include business process improvements, applying timely patches, configuring systems securely, performing secure application code development, and implementing architecture and design modifications as necessary. Risk mitigation measures will be employed based on prioritization. Some of the risk prioritization assessment criteria may include the probability of vulnerability exploitation, material business impact if vulnerability is successfully exploited, compliance requirements, cost and business impact of remediation activities and controls.

Specific categories of risks as described below may be accepted.

Acceptance of Risk (AOR) Letters. AOR letters are intended for rare or unusual circumstances where the System Owner has limited or no control over the remediation of an identified vulnerability. Examples of such circumstances include:

- Embedded software dependencies;
- Commercial off-the-shelf (COTS) product update timelines;
- Compatibility issues between components;
- Underlying GSS/platform issues that a system cannot remediate; and
- Contractual issues that prohibit remediation.
- Vulnerabilities in the CISA KEV that cannot be readily corrected.

Note: Due to the significant risk the KEVs pose to the federal government, AORs will only be authorized with CISO, CIO, and AO approval for no longer than 60 days from the KEV's due date. AOR requests should only be submitted based on an operational risk outweighing the security risk. No extensions will be offered for KEV associated AORs

AORs are not intended for:

- Delayed or ineffective flaw remediation processes (e.g., patching, addressing known vulnerabilities);
- Insufficient out-year System Development Life Cycle planning (for legacy components);
- System Owner preferences not supported by OCISO guidance and policies;

AOR requests must include mitigating factors, compensating controls, and any other action(s) taken to reduce the risk to the system and its data, and a justification for why the vulnerability cannot be resolved. The maximum duration of an AOR letter is one year. However, the duration should be only for as long as is necessary to remediate the vulnerabilities/findings for which the letter is being prepared (e.g., if remediation will

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

only take 3 months the duration should be 3 months). If remediation cannot be completed within the duration of the AOR letter, a new AOR letter must be prepared. The new AOR letter must include new/current details as to why the vulnerabilities/findings were not able to be remediated and the risk description revised, as necessary. Because the resolution exceeded the original AOR letter duration, the IST Director must discuss the rationale for the new AOR letter with the CISO. Evidence of this discussion (date, etc. must be documented in the AOR letter).

Based on the criteria above, AOR letters are:

- Not required for Very Low/Low risk vulnerabilities and findings.
- Required for Moderate risk vulnerabilities and findings. Moderate risk AOR letters require AO approval, but not CISO concurrence.
- Required for Critical/Very High/High risk vulnerabilities and findings. Critical/Very High/High risk AOR letters require AO approval and CISO concurrence.
- Required for any CISA KEV that cannot be readily corrected.

AOR Letter Processing. AOR letters are processed in the following manner:

1. The System Owner/Custodian, ISSO, and ISSM determine the need for an AOR letter.
2. The ISSO in conjunction with the ISSM prepares the AOR letter, including creation of an AOR ID# as specified below. NN is a sequential number of the AOR, YYYY is the current Fiscal Year, the brackets are not part of the AOR ID#.

   AOR-NN-[System Acronym]-YYYY Example: AOR-02-EIO-2021

3. The ISSM coordinates with the Director of IST to determine if a review discussion is appropriate with stakeholders and/or the CISO. If a review discussion is required, they jointly schedule the discussion and update the letter, if necessary.
4. The ISSM submits the AOR letter to:
   a. AO for approval of any Moderate risk AORs.
   b. AO for approval and CISO for concurrence for any Critical/Very High and High risk AORs.
5. Approved AOR letters are part of the permanent A&A files maintained by the ISSO and ISSM. AOR letters must be uploaded into the corresponding FISMA system's Archer GRC A&A Repository and an email sent to ispcompliance@gsa.gov indicating an AOR letter has been uploaded.
6. The ISSO is responsible for monitoring POA&Ms and AOR letters. When an AOR is within 30 days of expiring:
   a. If any POA&Ms listed in the AOR letter will not be resolved, a new AOR letter is required as described above.
   b. If all POA&Ms have been, or will be resolved prior to AOR letter expiration, then after all POA&Ms have been resolved the AOR letter is noted as completed and archived as a historical record of the system's A&A status.

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

7. AORs are reviewed on a monthly basis by the OCISO ISP Division. Any issues or pending deadlines are coordinated with the appropriate personnel.

5.7.4 TASK M-4: Authorization Package Updates

The System Owner and ISSO will update the following items as part of the system and GSA continuous monitoring plans, processes, and program.

- SSPP (and all appendices and attachments);
- POA&M.

The updates will be based on regular updates required by GSA processes, such as:

- Vulnerability scans from GSA's scanning program;
- Annual FISMA self-assessments;
- Penetration tests;
- Audits, or related assessments;
- Changes identified as part of a system's CM Plan;
- For systems in the GSA OA Program, performance metrics established as part of ongoing authorization per CIO-IT Security-12-66.

As part of the CM process outlined within CIO-IT Security-01-05, security testing will be conducted following major or significant system changes. If the changes introduce vulnerabilities, actions to mitigate the vulnerabilities must be included in the system's POA&M, per GSA's POA&M management process, for tracking of the resolution. The SSPP will be updated to reflect any changes.

5.7.5 TASK M-5: Security and Privacy Reporting

The System Owner and ISSO will report the security and privacy status of the information system (including the effectiveness of security and privacy controls employed within and inherited by the system) to the AO and other appropriate organizational officials on an ongoing basis. GSA's vulnerability management program, the POA&M management process, privacy program, and any required reporting processes/capabilities (e.g., FISMA, OA, CDM) will be used to provide security and privacy status reporting. AOs and other personnel with security and privacy related responsibilities will leverage these resources to keep apprised of the risk levels associated with GSA's system(s).

5.7.6 TASK M-6: Ongoing Authorization

GSA's OA Program as described in CIO-IT Security-12-66 relies on GSA's continuous monitoring strategy. That strategy leverages both manual and automated processes to monitor a system's security and privacy controls. The objective of the strategy is to ensure all key information security and privacy controls are periodically assessed for effectiveness. It leverages GSA's deployment of CDM and other Enterprise Security Management tools to monitor the security of GSA's systems. CIO-IT Security-12-66 provides more details on how GSA continuously monitors vulnerabilities, threats, and actions taken to reduce, mitigate, or eliminate them. Key components of GSA's strategy are regular vulnerability scanning activities and security

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

configuration checks, the requirement to maintain A&A documents in an "as-is" state, management and review of POA&Ms, and ISSO Checklists within Archer GRC.

In order to enter into the OA Program systems must meet prerequisites defined in CIO-IT Security-12-66 and successfully complete the onboarding process which includes completion of a checklist verifying the security status of the system, review of GSA's OA and showstopper controls, review of system artifacts, verifying that GSA security tools are in place and monitoring the system. The GSA OA Team coordinates with System Owner, ISSM, and ISSO during the onboarding process and semi-annual performance reviews for systems in the OA Program.

5.7.7 TASK M-7: System Disposal

System Owners and ISSOs must manage systems from inception through disposal in accordance with CIO Order 2140.4, "*Information Technology (IT) Solutions Life Cycle (SLC) Policy*." In support of system disposal system owners will document the transfer and/or disposal of GSA IT Systems using GSA's Transfer and Disposal Notification Templates and in accordance with the provisions outlined within CIO 2100.1.

5.8 A&A Guidance for Significant Changes

Significant changes as defined in NIST SP 800-37, Appendix F, require reauthorization following the security authorization process requirements in this guide. Contact the OCISO at ispcompliance@gsa.gov to determine the scope of reauthorization activities.

5.9 A&A Guidance for Expiring Authorizations

ISSOs, ISSMs, and the IST Director can track the expiration dates of ATOs using GSA's implementation of Archer GRC. Renewals of ATOs are initiated by the Authorizing Officials, ISSMs, and ISSOs. Per Chapter 3, Section 3, Governance, of GSA CIO 2100.1:

> *m. Extension of a system's current ATO for a period not to exceed one year (365 days) may only be requested under one of the following conditions. The system must continue to maintain its complete set of A&A documentation (e.g., System Security Plan, Contingency Plan, POA&Ms). All actions to satisfy the conditions below must be completed within the extension period (i.e., no longer than 12 months).*
>
> *(1) Transitioning to ongoing authorization;*
> *(2) Planning for disposal;*
> *(3) Consolidating into another system for its ATO. The scope of consolidation shall be approved by the OCISO prior to submitting the ATO extension request;*
> *(4) Transitioning into a cloud environment for its ATO. The scope of the transition into the cloud environment shall be approved by the OCISO prior to submitting the ATO extension request;*
> *(5) Re-competing the system's contract;*

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

(6) Completing the upgrade/replacement of major infrastructure components;
(7) Completing the system's security assessment has been delayed due to contract issues; or
(8) Complying with Showstopper controls as listed in CIO-IT Security-06-30.

n. An information system undergoing a three-year re-authorization having outstanding high or very high/critical vulnerabilities identified during its security assessment, may request a one-time extension for a period not to exceed thirty (30) days from the date of the ATO expiry to allow mitigation of the high and very high/critical vulnerabilities. No more than two extensions may be granted under this condition.

Note: The CISO may also grant extensions on a case-by-case basis due to extenuating circumstances.

Questions concerning the security authorization process, significant changes, or expiring ATOs can be directed to your designated ISSM.

6 Protecting Confidential Unclassified Information (CUI) in Nonfederal Systems and Organizations

GSA CIO-IT Security-21-112, "Protecting Controlled Unclassified Information (CUI) in Nonfederal Systems and Organizations Process," is being developed and will define the processes and procedures that will be used to ensure nonfederal systems protect CUI in accordance with the requirements of NIST SP 800-171, Revision 2, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations." The requirements identified in both documents are applicable under the following conditions:

- CUI is resident in a nonfederal system and organization;
- the nonfederal organization is not collecting or maintaining information on behalf of a federal agency or using or operating a system on behalf of an agency;[2] and
- there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or governmentwide policy for the CUI category listed in the CUI Registry.[3]

The requirements apply only to components of nonfederal systems that process, store, or transmit CUI, or that provide security protection for such components.

[2] Nonfederal organizations that collect or maintain information *on behalf of* a federal agency or that use or operate a system *on behalf of* an agency, must comply with the requirements in the Federal Information Security Modernization Act (FISMA), including the requirements in [FIPS 200] and the security controls in [SP 800-53] (See [44 USC 3554] (a)(1)(A)).

[3] The requirements in NIST SP 800-171 can be used to comply with the [FISMA] requirement for senior agency officials to provide information security for the information that supports the operations and assets under their control, including CUI that is resident in nonfederal systems and organizations (See [44 USC 3554] (a)(1)(A) and (a)(2)).

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

7 Independent Assessment of Enterprise-wide Common and Hybrid Controls

CIO-IT Security-18-90, fulfills the requirement for a security program per NIST SP 800-53, Control PM-1, Information Security Program Plan. NIST SP 800-37, requires that common controls be assessed and authorized. The controls in the ISPP (both common and the common portion of hybrid controls) are assessed at least every three (3) years and authorized for use similar to any system as described in Sections 5.5 and 5.6.

8 GSA Implementation of CA, PL, and RA Controls

NIST SP 800-53 defines controls related to the security authorization process that GSA is required to implement based on an information system's security categorization. The Assessment, Authorization, and Monitoring (CA), Planning (PL), and Risk Assessment (RA) control family implementations are addressed in this guide. Only those controls applicable at any FIPS 199 Level in accordance with NIST SP 800-53B are included in this section.

8.1 Assessment, Authorization, and Monitoring (CA)

8.1.1 CA-1 Policy and Procedures

Control:

a. Develop, document, and disseminate to [*personnel with IT security responsibilities as defined in GSA CIO Order 2100.1*]:
    1. [*Organization-level*] assessment, authorization, and monitoring policy that:
        (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
        (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
    2. Procedures to facilitate the implementation of the assessment, authorization, and monitoring policy and the associated assessment, authorization, and monitoring controls;
b. Designate an [*CISO*] to manage the development, documentation, and dissemination of the assessment, authorization, and monitoring policy and procedures; and
c. Review and update the current assessment, authorization, and monitoring:
    1. Policy [*annually, as part of CIO 2100.1, GSA IT Security Policy*] and following [*changes to Federal or GSA policies, requirements, or guidance*]; and
    2. Procedures [*at least every three (3) years*] and following [*changes to Federal or GSA policies, requirements, or guidance*].

GSA Implementation Guidance:

The GSA security assessment and authorization policy is defined in the GSA IT Security Policy, CIO 2100.1, which addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance regarding assessing and

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

authorizing systems for GSA. This policy is disseminated GSA-wide via GSA's InSite centralized agency website.

Security assessment and authorization procedures are documented in this guide. Additional security and assessment guides for specific types of systems have been developed and are referenced in this guide. The procedures in these guides facilitate the security assessment and authorization of all GSA systems. The guides are disseminated GSA-wide via GSA's InSite centralized agency website.

The GSA CISO is responsible for managing the development, documentation, and dissemination of the policies and procedures for GSA IT.

The GSA OCISO is responsible for reviewing and updating CIO 2100.1 annually.

The GSA OCISO is responsible for reviewing and updating CIO-IT Security 06-30 at least every three (3) years and following changes to Federal or GSA policies, requirements, or guidance.

Additional Contractor System Considerations: *Vendors/contractors must adhere to GSA's policy and guide regarding the security assessment and authorization of GSA systems.*

8.1.2 CA-2 Control Assessments

Control:

a. Select the appropriate assessor or assessment team for the type of assessment to be conducted
b. Develop a control assessment plan that describes the scope of the assessment including:
    1. Controls and control enhancements under assessment;
    2. Assessment procedures to be used to determine control effectiveness; and
    3. Assessment environment, assessment team, and assessment roles and responsibilities;
c. Ensure the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment;
d. Assess the controls in the system and its environment of operation [*annually*] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements;
e. Produce a control assessment report that document the results of the assessment; and
f. Provide the results of the control assessment to [*personnel with system security responsibilities as identified in CIO 2100.1 and CIO-IT Security 06-30*].

Control Enhancements:

(1) Control Assessments | Independent Assessors – Employ independent assessors or assessment teams to conduct control assessments.
Note: *Assessors are independent if they do not: (i) have a mutual or conflicting interest with the organizations where the assessments are being conducted; (ii) assess their own work; (iii) act as management or employees of the organizations they are assessing; or*

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

(iv) place themselves in positions of advocacy for the organizations acquiring their services.

(2) Control Assessments | Specialized Assessments – Include as part of control assessments [*annual*], [*announced*], [*penetration testing*].

GSA Implementation Guidance:
GSA requires a security control assessment to be performed is defined in Section 5.5 of this guide. The tasks in that section include the selection of the appropriate assessors, the development of an assessment plan identifying the controls to be assessed, the procedures to be used, the team, environment, and roles and responsibilities. The plan is required to be approved before the assessment can begin. The execution of the assessment plan and the preparation of the assessment report is described, including the report being part of the A&A package that is provided to the ISSM, CISO, System Owner, and AO.

As per CA-2, Enhancement (1), GSA FIPS 199 Moderate and High Impact Systems must be assessed by an independent third party. All FIPS 199 Low external vendor/contractor systems must be assessed by an independent third party. The use of an independent assessment team reduces the potential for impartiality or conflicts of interest when verifying the implementation status and effectiveness of the security controls.

As per CA-2, Enhancement (2), GSA FIPS 199 High Impact Systems must be assessed annually via announced penetration tests. Penetration testing provides a more thorough analysis of the implementation effectiveness of security controls associated with an information system.

Additional Contractor System Considerations: *Vendors/contractors must adhere to GSA's policy and the controls regarding the security assessment of GSA systems.*

8.1.3 CA-3 Information Exchange

Control:

a. Approve and manage the exchange of information between the system and other systems using [*interconnection security agreements as applicable per 06-30 and documented in the system's SSPP interconnection section (Tables 11-1 and 11-2)*];
b. Document, as part of each exchange agreement, the interface characteristics, security and privacy requirements, controls, and responsibilities for each system, and the impact level of the information communicated; and
c. Reviews and updates Interconnection Security Agreements [*at least annually*].

Control Enhancements:

(6) Information Exchange | Transfer Authorizations – verify that individuals or systems transferring data between interconnecting systems have the requisite authorizations (i.e., write permissions or privileges) prior to accepting such data.

GSA Implementation Guidance:
The focus of this control is to ensure that any persistent connection to any other information system outside of the system's authorization boundary has been approved by the AO, identified and documented within the SSPP, and monitored on an ongoing basis.

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

GSA CIO 2100.1 outlines the following interconnection requirements:

Chapter 3
1.d All interconnections between GSA and external entities including off-site contractors or Federal agency/departments must be documented in an Interconnection Security Agreement (ISA) that is approved by the AOs and concurred by the GSA CISO. ISA's must, at a minimum, be reviewed annually. See NIST SP 800-47[4], Security Guide for Interconnecting Information Technology Systems for detailed information.

1.f All system interconnections, including connections to external systems, must be documented in a system's SSPP.

Chapter 4
6.o. If GSA systems interconnect, they must connect using a secure methodology that provides security commensurate with the acceptable level of risk as defined in the system security plan and that limits access only to the information needed by the other system IAW GSA CIO-IT Security-01-07 and GSA CIO-IT Security-06-30. All interconnections between GSA and external entities including off-site contractors or Federal agency/departments must be approved by the GSA CISO.

Per NIST 800-47, an interconnection is the direct connection of two or more IT systems for the purpose of sharing data and other information resources through a pipe, such as ISDN, T1, T3, DS3, VPN, API, etc. The terms "connection" or "interconnection" in this case, means any on-going, persistent, or substantial interaction with any information system(s) that is located outside of the authorization boundary. These connections can be physical and/or logical and include data entering or exiting to/from the authorization boundary. User-controlled connections such as email, ftp, remote access, and web browsing are not considered interconnections and therefore do not apply to this control.

As per CA-3, Enhancement (6), GSA FIPS 199 High Impact Systems must ensure the appropriate authorizations (i.e., write permissions or privileges) between the individuals or systems transferring data between the interconnecting systems have been verified prior to accepting such data.

Additional Contractor System Considerations: *Vendors/contractors must adhere to GSA policies and guides and the control requirements*.

8.1.4 CA-5 Plan of Action and Milestones

Control:

a. Develop a plan of action and milestones for the system to document the planned remediation actions of the organization to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system; and

[4] NIST has issued NIST SP 800-47, Revision 1, *"Managing the Security of Information Exchanges,"* CIO 2100.1 will be updated to reflect Revision 1.

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

b. Update existing plan of action and milestones [*at least quarterly*] based on the findings from control assessments, independent audits or reviews, and continuous monitoring activities.

GSA Implementation Guidance:
The focus of this control is to ensure that all information systems have developed a POA&M in accordance with CIO-IT 09-44 which details the POA&M processes and procedures for meeting the requirements of this control.

On a quarterly basis, POA&Ms will be reviewed by the OCISO in order to monitor agency-wide remediation efforts as required by OMB policy. Updates to POA&Ms should be performed by the ISSO as milestones or actions occur throughout the fiscal year. POA&Ms are located on individual system POA&M Share Drives and are maintained by the system ISSO or ISSM. The POA&M Shared Drives serve as the primary location for managing and communicating GSA's system and program POA&Ms, and are available internally at GSA, or via VPN. New systems that are currently undergoing a security authorization process or that have not been included in the GSA FISMA inventory must use the POA&M Template available on the POA&M Guidance Shared Drive or by contacting ispcompliance@gsa.gov.

Additional Contractor System Considerations:
Contractor systems must provide POA&Ms through their ISSO(s) as contractors will not have access to the POA&M Shared Drives. ISSOs supporting these systems must facilitate POA&M updates by sending the current version of the system POA&M together with the OCISO guidance to the contractor representative(s). Upon receipt of the POA&M from the contractor, ISSOs shall review the POA&M to ensure it is updated and includes required vulnerabilities before updating the POA&M on the GSA POA&M Shared Drives.

8.1.5 CA-6 Authorization

Control:

a. Assign a senior official as the authorizing official for the system;
b. Assign a senior official as the authorizing official for common controls available for inheritance by organizational systems;
c. Ensure that the authorizing official for the system, before commencing operations:
    1. Accepts the use of common controls inherited by the system; and
    2. Authorizes the system to operate;
d. Ensure that the authorizing official for common controls authorizes the use of those controls for inheritance by organizational systems;
e. Update the authorizations [*as specified in CIO-IT Security-06-30 and GSA's other Assessment and Authorization processes identified therein*].

GSA Implementation Guidance:
The focus of this control is to ensure all information systems have been authorized to operate before being placed into operational status. All information systems adhering to the GSA Standard A&A process must undergo authorization/reauthorization every three years or when there is a significant change as defined in NIST SP 800-37, Appendix F, following the security

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

authorization process documented in Section 5 of this guide, RMF Assess Step. Additional A&A or authorization types exist in GSA and are described in Section 4 of this document.

The explicit acceptance of *risk* is the responsibility of the AO. The AO must consider many factors, balancing security considerations with mission and operational needs. The AO issues an authorization decision for the information system and the common controls inherited by the system after reviewing the security authorization package submitted by the System Owner. The security authorization package provides the AO with the essential information needed to make a credible risk-based decision on whether to authorize operation of the information system.

For GSA's Standard A&A process, the security authorization package includes:

- SSPP (with all appendices and attachments);
- Security Assessment Report (with all appendices and attachments);
- POA&M;
- Certification Memorandum;
- ATO Letter.

Note: The documents outlined for the Security Authorization Package (above) are required for the GSA Standard A&A Process. The documentation required and links to document templates for other A&A processes GSA uses (and the standard process) are listed in Appendix C.

The AO must determine if the remaining known vulnerabilities in the information system pose an acceptable level of risk to agency operations, assets, and individuals and determine if the risk to the agency is acceptable. Following review of the security authorization package and consultation with key agency officials, the AO must render an authorization decision to:

- Authorize system operation without any restrictions or limitations on its operation;
- Authorize system operation with restrictions/limitations on its operations. The POA&M must include detailed corrective actions to correct the deficiencies requiring the restrictions/limitations. The ISSM/ISSO must resubmit an updated authorization package upon completion of required POA&M actions to move to a full ATO without any restrictions/limitations; or
- Not authorize the system for operation.

Authorization of common controls at the enterprise level are indicated by the GSA CISO signing the ISPP where enterprise common controls are documented. Authorization of common controls provided by systems to other systems is indicated when AOs sign the ATO Letter for the system providing common controls.

Questions concerning the security authorization process, significant changes, or CIO 2100.1 can be directed to ispcompliance@gsa.gov.

Additional Contractor System Considerations: *Vendors/contractors must adhere to GSA policies and guides and the control requirements*.

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

8.1.6 CA-7 Continuous Monitoring

Control:

Develop a system-level continuous monitoring strategy and implement continuous monitoring in accordance with the organization-level continuous monitoring strategy that includes:

a. Establishing the following system-level metrics to be monitored: [*as specified in Section 3 of CIO-IT Security-08-39, Management Implementation Plan and CIO-IT Security-12-66, ISCM Strategy and OA Program*];
b. Establishing [*frequencies as specified in Section 3 of CIO-IT Security-08-39, Management Implementation Plan and CIO-IT Security-12-66, ISCM Strategy and OA Program*] for monitoring and [*frequencies as specified in Section 3 of CIO-IT Security-08-39, Management Implementation Plan and CIO-IT Security-12-66, ISCM Strategy and OA Program*] for assessment of control effectiveness;
c. Ongoing control assessments in accordance with the continuous monitoring strategy;
d. Ongoing monitoring of system and organization-defined metrics in accordance with the continuous monitoring strategy;
e. Correlation and analysis of information generated by control assessments and monitoring;
f. Response actions to address results of the analysis of control assessment and monitoring information; and
g. Reporting the security and privacy status of the system to [*CISO, AOs, System Owners, ISSMs, ISSOs, Custodians*] [*as specified in CIO-IT Security-08-39, Management Implementation Plan and CIO-IT Security-12-66, ISCM Strategy and OA Program*].

Control Enhancements:

(1) Continuous Monitoring | Independent Assessment – Employ independent assessors or assessment teams to monitor the controls in the system on an ongoing basis.
NOTE: *Independence is waived for all annual testing (i.e., testing can be internally performed).*

(4) Continuous Monitoring | Risk Monitoring – Ensure risk monitoring is an integral part of the continuous monitoring strategy that includes the following:
    (a) Effectiveness monitoring;
    (b) Compliance monitoring; and
    (c) Change monitoring.

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

GSA Implementation Guidance:
GSA OCISO has established continuous monitoring frequencies for metrics in CIO-IT Security-08-39, Management Implementation Plan and CIO-IT Security-12-66, ISCM Strategy and OA Program. GSA OCISO requires systems to complete an annual FISMA Self-Assessment (unless a full assessment has been completed) in addition to the use of Continuous Diagnostics and Mitigation (CDM) and other Enterprise Security Management tools to continually assess the security status of systems. GSA leverages its deployment of CDM and other Enterprise Security Management tools, their dashboards, and reports to correlate findings and analyze them. System owners, ISSOs, ISSMs, and system personnel are responsible for addressing findings from annual assessments and results from GSA's CDM and other Enterprise Security Management tools in accordance with CIO-IT this guide and CIO-IT Security-17-80. GSA leverages its deployment of CDM and other Enterprise Security Management tools, their dashboards, and reports to inform personnel with security responsibilities for systems the status of their systems in accordance with CIO-IT Security-06-30 and CIO-IT Security-17-80.

As per CA-7, Enhancement (2), GSA FIPS 199 Moderate and High Impact Systems must be assessed by an independent third party. The use of an independent assessor/assessment team reduces the potential for impartiality or conflicts of interest, when verifying the implementation status and effectiveness of the security controls.

As per CA-7, Enhancement (4), GSA FIPS 199 Low, Moderate, and High Impact Systems must use manual and automated processes to monitor security and privacy controls. GSA's organizational continuous monitoring strategy leverages its deployment of CDM and other Enterprise Security Management tools to monitor the security of GSA's systems. CIO-IT Security-08-39 and CIO-IT Security-12-66 provide more details on how GSA continuously monitors for vulnerabilities, threats, and actions taken to reduce, mitigate, or eliminate them. Key components of GSA's strategy are regular vulnerability scanning activities and security configuration checks, the requirement to maintain A&A documents in an "as-is" state, management and review of POA&Ms, and ISSO Checklists within Archer GRC. Per CIO-IT Security-01-05, proposed system changes must be evaluated to determine potential security impacts.

Additional Contractor System Considerations: *Vendors/contractors must adhere to GSA policies and guides and the control requirements.*

8.1.7 CA-8 Penetration Testing

Control:
Conduct penetration testing [*during A&A efforts and annually thereafter*] on [*all Internet accessible, FIPS 199 High impact, and High Value Asset (HVA) information systems*].

Control Enhancements:

(1) Penetration Testing | Independent Penetration Testing Agent or Team - Employ an independent penetration agent or penetration team to perform penetration testing on the information system or system components.

NOTE: *Independence is waived for all annual testing (i.e., testing can be internally performed).*

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

GSA Implementation Guidance:
All Internet accessible, FIPS 199 High impact, and HVA information systems are required to complete an independent penetration test and provide a Penetration Test Report documenting the results of the exercise as part of the A&A package. Annual penetration tests can be completed internally and do not require an independent assessor. Penetration testing will be conducted in accordance with CIO-IT Security-11-51, including the use of a sampling of web applications based on FIPS 199 security impact levels and the selection of FISMA systems subject to the GSA Annual Penetration Test.

Additional Contractor System Considerations: *Vendor/contractor systems must comply with the controls IAW the guidance and control parameters established above.*

8.1.8 CA-9 Internal System Connections

Control:

a. Authorize internal connections of [*other GSA components using a secure methodology providing security commensurate with the acceptable level of risk as defined in the SSPP and limits access to the information needed by the connected component*] to the system;
b. Document, for each internal connection, the interface characteristics, security and privacy requirements, and the nature of the information communicated;
c. Terminate internal system connections after [*15 minutes of inactivity for non-persistent connections*]; and
d. Review [*annually (or as the SSPP is reviewed and updated)*] the continued need for each internal connection.

GSA Implementation Guidance:
If GSA systems interconnect, they must connect using a secure methodology that provides security commensurate with the acceptable level of risk as defined in the system security plan and that limits access only to the information needed by the other system.

8.2 Planning (PL)

8.2.1 PL-1 Policy and Procedures

Control:

a. Develop, document, and disseminate to [*personnel with IT security responsibilities as defined in GSA CIO Order 2100.1*]:
    1. [*Organization-level*] planning policy that:
        (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
        (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
    2. Procedures to facilitate the implementation of the planning policy and the associated planning controls;
b. Designate an [*CISO*] to manage the development, documentation, and dissemination of the planning policy and procedures;

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

c. Review and update the current planning:
    1. Policy [*annually, as part of CIO 2100.1, GSA IT Security Policy*] and following [*changes to Federal or GSA policies, requirements, or guidance*]; and
    2. Procedures [*at least every three (3) years*] and following [*changes to Federal or GSA policies, requirements, or guidance*].

GSA Implementation Guidance:
The GSA security planning policy is defined in the GSA IT Security Policy, CIO 2100.1, which addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance regarding security planning for GSA systems. This policy is disseminated GSA-wide via GSA's InSite centralized agency website.

GSA security planning procedures are documented in this guide, including the identification of additional security and assessment guides for specific types of systems. The procedures and processes in these guides facilitate the implementation of the GSA's security policy and assessment and authorization processes. All GSA guides are disseminated GSA-wide via GSA's InSite centralized agency website.

The GSA CISO is responsible for managing the development, documentation, and dissemination of the policies and procedures for GSA IT.

The GSA OCISO is responsible for reviewing and updating CIO 2100.1 annually.

The GSA OCISO is responsible for reviewing and updating CIO-IT Security 06-30 at least every three (3) years and following changes to Federal or GSA policies, requirements, or guidance.

Additional Contractor System Considerations: *Vendors/contractors may defer to the GSA policy and guide or implement their own security planning policies and procedures which comply with GSA's requirements with the approval of the CISO and AO.*

8.2.2 PL-2 System Security and Privacy Plans

Control:

a. Develop security and privacy plans for the system that:
    1. Are consistent with the organization's enterprise architecture;
    2. Explicitly define the constituent system components;
    3. Describe the operational context of the system in terms of mission and business processes;
    4. Identify the individuals that fulfill system roles and responsibilities;
    5. Identify the information types processed, stored, and transmitted by the system;
    6. Provide the security categorization of the system, including supporting rationale;
    7. Describe any specific threats to the system that are of concern to the organization;
    8. Provide the results of a privacy risk assessment for systems processing personally identifiable information;

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

9. Describe the operational environment for the system and any dependencies on or connections to other systems or system components;
10. Provide an overview of the security and privacy requirements for the system;
11. Identify any relevant control baselines or overlays, if applicable;
12. Describe the controls in place or planned for meeting the security and privacy requirements, including a rationale for any tailoring decisions;
13. Include risk determinations for security and privacy architecture and design decisions;
14. Include security- and privacy-related activities affecting the system that require planning and coordination with [*personnel with IT security responsibilities for the system as defined in GSA CIO Order 2100.1 and the GSA Privacy Office (for systems with Privacy Act data)*]; and
15. Are reviewed and approved by the authorizing official or designated representative prior to plan implementation.

b. Distribute copies of the plans and communicate subsequent changes to the plans to [*personnel with IT security responsibilities for the system as defined in GSA CIO Order 2100.1*];
c. Review the plans [*annually*];
d. Update the plans to address changes to the system and environment of operation or problems identified during plan implementation or control assessments; and
e. Protect the plans from unauthorized disclosure and modification

GSA Implementation Guidance:
The focus of this control is to ensure that an SSPP has been developed for the information system that documents the security requirements for the information system, and the implementation status of the security controls that have been assigned to the system as per FIPS 199 impact analysis. All GSA information systems must develop an SSPP when required by GSA's A&A processes described in this guide using GSA SSPP templates based on NIST SP 800-18. Detailed guidance is available through Section 5 of this guide.

The security requirements per FIPS 199 impact level and the security controls which are planned or in-place to meet these requirements, must be documented within the SSPP and updated as-needed to reflect any change to the information system environment. Updates made to the SSPP must include updates to system applications and hardware, remediation of previously identified weaknesses and any addition of new weaknesses identified through security assessments or continuous monitoring.

Systems must include in their SSPP a section on transitioning to IPv6. Systems following AWS and DevOps/DevSecOps practices must include in their SSPP, or a supplemental document, security practices used to manage their environment and deployment processes.

Additional Contractor System Considerations: *Vendors/contractors must adhere to GSA policies and guides and the control requirements*.

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

8.2.3 PL-4 Rules of Behavior

Control:

a. Establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy;
b. Receive a documented acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the system;
c. Review and update the rules of behavior [*at least annually*]; and
d. Require individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge [Selection (one or more): [*annually or when the rules are revised or updated*].

Control Enhancements:

(1) Rules of Behavior | Social Media and External Site/Application Usage Restrictions - Include in the rules of behavior, restrictions on:
    (a) Use of social media, social networking sites, and external sites/applications;
    (b) Posting organizational information on public websites; and
    (c) Use of organization-provided identifiers (e.g., email addresses) and authentication secrets (e.g., passwords) for creating accounts on external sites/applications

GSA Implementation Guidance:

GSA has developed the GSA IT Rules of Behavior for General Users as indicated in CIO-IT Security-05-029, "Security and Privacy Awareness and Role Based Training Program." The rules describe a user's responsibilities and expected behavior when using GSA information systems including use of social media and external sites/applications, posting organizational information on public websites, and using organizational identifiers or authentication secrets when creating accounts on external sites/applications. All GSA IT users must sign the GSA IT General Rules of Behavior for General Users within 90 days of their entry on duty (EoD). Based on risk-based decision for operational reasons, GSA does not require the rules be signed before accessing an information system. GSA OCISO reviews and updates the GSA IT Rules of Behavior for General Users annually. All GSA IT users are required to re-sign the GSA IT Rules of Behavior for General Users annually or when the rules are revised or updated as part of GSA's annual IT Security and Privacy Awareness training.

As per PL-4, Enhancement (1), GSA Order CIO 2100.1, "GSA Information Technology (IT) Security Policy," provides basic restrictions on the use of social media/networking. GSA Order OSC 2106.2, "GSA Social Media Policy," provides detailed instructions regarding what GSA personnel can and cannot do regarding the use of social media/networking.

Additional Contractor System Considerations: *Vendors/contractors must adhere to the control requirements and may defer to the GSA rules of behavior or may augment them with their own rules of behavior.*

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

8.2.4 PL-8 Information Security Architecture

Control:

a. Develop security and privacy architectures for the system that:
   1. Describe the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of organizational information;
   2. Describe the requirements and approach to be taken for processing personally identifiable information to minimize privacy risk to individuals;
   3. Describe how the architectures are integrated into and support the enterprise architecture; and
   4. Describe any assumptions about, and dependencies on, external systems and services;

b. Review and update the architectures [*as necessary, and at least annually in conjunction with SSPP reviews/updates*] to reflect changes in the enterprise architecture; and

c. Reflect planned architecture changes in security and privacy plans, Concept of Operations (CONOPS), criticality analysis, organizational procedures, and procurements and acquisitions.

GSA Implementation Guidance:

GSA CIO-IT Security-19-95, "Security Engineering Architecture Reviews" describes GSA's processes for ensuring systems are built in accordance with the Security Engineering Framework to meet GSA's security requirements and protect GSA systems and data. It includes checklist items that ensure a system's security architecture aligns with GSA's Enterprise Architecture and protects sensitive data, including personally identifiable information. The checklist includes items regarding the use of external services, systems, and interconnections.

CIO-IT Security-19-95 describes the process for ensuring systems are designed and built securely when systems undergo major architectural changes. The system ISSO has the responsibility to notify the ISE Division when changes occur and, as part of the system's SSP annual update, to consider if any changes have occurred that require architectural review. The system ISSO also has the responsibility to ensure any security architecture changes are reflected in the system's SSP. The ISE Division coordinates with the Enterprise Architecture Review Committee to approve new IT standards which can then be included in procurements/acquisitions.

Additional Contractor System Considerations: *Vendors/contractors must adhere to GSA policies and guides and the control requirements*.

8.2.5 PL-9 Central Management

Control:

Centrally manage [*common and hybrid security and privacy controls as identified in CIO-IT Security-18-90, Information Security Program Plan (ISPP)*].

GSA Implementation Guidance:

Enterprise common and hybrid controls are described in the ISPP. GSA system owners, data owners, ISSOs, and ISSMs are responsible for coordinating the inheritance of controls identified

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

in the ISPP for their FISMA systems. For hybrid controls, they must implement the system specific portions of the controls as described in the ISPP.

Additional Contractor System Considerations: *Expectations for vendor/contractor systems are specified in the ISPP. Most of the controls in the ISPP are system-specific or hybrid for vendor/contractor systems, therefore central management of those controls is the responsibility of the vendor/contractor.*

8.2.6 PL-10 Baseline Selection

Control:
Select a control baseline for the system.

GSA Implementation Guidance:
GSA system owners, data owners, ISSOs, and ISSMs are required to follow the processes and procedures described in Section 5.3.1 of this guide for selecting the control baseline for their information and information systems.

Additional Contractor System Considerations: *Vendor/contractor systems must follow the same processes and procedures for selecting a control baseline as described in Section 5.3.1.*

8.2.7 PL-11 Baseline Tailoring

Control:
Tailor the selected control baseline by applying specified tailoring actions.

GSA Implementation Guidance:
GSA system owners, data owners, ISSOs, and ISSMs are required to follow the processes and procedures described in Section 5.3.2 for determining the tailored actions of their information and information systems baseline(s).

Additional Contractor System Considerations: *Vendor/contractor systems must follow the same processes and procedures for baseline tailoring as described in Section 5.3.2.*

8.3 Risk Assessment (RA)

8.3.1 RA-1 Policy and Procedures

Control:

a. Develop, document, and disseminate to [*personnel with IT security responsibilities as defined in GSA CIO Order 2100.1*]:
    1. [*Organization-level*] risk assessment policy that:
        (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
        (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

2. Procedures to facilitate the implementation of the planning policy and the associated risk assessment controls;

b. Designate an [*CISO*] to manage the development, documentation, and dissemination of the risk assessment policy and procedures; and
c. Review and update the current risk assessment:
    1. Policy [*annually, as part of CIO 2100.1, GSA IT Security Policy*] and following [*changes to Federal or GSA policies, requirements, or guidance*]; and
    2. Procedures [*at least every three (3) years*] and following [*changes to Federal or GSA policies, requirements, or guidance*].

GSA Implementation Guidance:
GSA's risk assessment policy is defined in the GSA IT Security Policy, CIO 2100.1, which addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance regarding risk assessment for GSA systems. This policy is disseminated GSA-wide via GSA's InSite centralized agency website.

GSA's risk assessment procedures are documented in this guide and other procedural guides referenced in it. The procedures facilitate the implementation of the risk assessment policy and associated controls. All GSA guides are disseminated GSA-wide via GSA's InSite centralized agency website.

The GSA CISO is responsible for managing the development, documentation, and dissemination of the policies and procedures for GSA IT. The GSA OCISO is responsible for reviewing and updating CIO 2100.1 annually. The GSA OCISO is responsible for reviewing and updating CIO-IT Security 06-30 at least every three (3) years and following changes to Federal or GSA policies, requirements, or guidance.

Additional Contractor System Considerations: *Vendors/contractors must use GSA policies and guides regarding risk assessment policies and procedures. They may supplement them with their own risk assessment policies and procedures with the approval of the GSA CISO and AO.*

8.3.2 RA-2 Security Categorization

Control:

a. Categorize the system and information it processes, stores, and transmits;
b. Document the security categorization results, including supporting rationale, in the security plan for the system; and
c. Verify that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.

GSA Implementation Guidance:
GSA system owners, data owners, ISSOs, and ISSMs are required to follow the processes and procedures described in Section 5.2.2 of this guide for determining the security categorization of their information and information systems.

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

Additional Contractor System Considerations: *Vendor/contractor systems must follow the same processes and procedures for determining the security categorization of their information and information systems as described in Section 5.2.2.*

8.3.3 RA-3 Risk Assessment

Control:

a. Conduct a risk assessment, including:
   1. Identifying threats to and vulnerabilities in the system;
   2. Determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; and
   3. Determining the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information;

b. Integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments;

c. Document risk assessment results in [*a security assessment report (SAR) or as specified in CIO-IT Security-06-30 and GSA's other Assessment and Authorization processes identified therein*];

d. Review risk assessment results [*as specified in CIO-IT Security-06-30 and GSA's other Assessment and Authorization processes identified therein*];

e. Disseminate risk assessment results to [*personnel with risk assessment/management responsibilities as defined in GSA CIO Order 2100.1*]; and

f. Update the risk assessment [*as specified in CIO-IT Security-06-30 and GSA's other Assessment and Authorization processes identified therein*] or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system.

Control Enhancements:

(1) Risk Assessment | Supply Chain Risk Assessment –
   (a) Assess supply chain risks associated with [*GSA S/SO or Contractor recommended systems, system components, and system services as approved by the CISO and AO*]; and
   (b) Update the supply chain risk assessment [*GSA S/SO or Contractor recommended frequency as approved by the CISO and AO*], when there are significant changes to the relevant supply chain, or when changes to the system, environments of operation, or other conditions may necessitate a change in the supply chain.

GSA Implementation Guidance:

The focus of this control is to verify that an assessment of risk is performed and documented for the information system and that the subsequent security assessment report is communicated to GSA senior management, in order to provide key information regarding the system's current security state and resulting risk to GSA operations, assets, and individuals. The results of the risk assessment provide critical information to assist the GSA AO in determining whether or not to authorize/re-authorize the information system.

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

GSA requires a risk assessment to be conducted as part of a system's initial security authorization process, and then risk is assessed in accordance with the specific GSA A&A process used from Section 4. GSA's process for performing a risk assessment is defined in Section 5.5.4 of this guide and in the GSA A&A processes listed in Section 4. The results of this risk assessment must be documented as defined in the GSA A&A process used.

As per RA-3, Enhancement (1), GSA FIPS 199 Low, Moderate, and High Impact Systems must coordinate with the GSA OCISO to identify systems, components, and services to be assessed for supply chain risk. The supply chain risk assessment must be updated at a mutually agreed upon time frame coordinated with the GSA CISO and AO. Systems must ensure the proscribed companies identified in CIO-IT Security-09-48 are not providing equipment, systems, or services for their systems or they have an exception or waiver per the Federal Acquisition Regulation.

Additional Contractor System Considerations: *Vendors/contractors must adhere to GSA policies and guides and the control requirements.*

8.3.4 RA-5 Vulnerability Monitoring and Scanning

Control:

a. Monitor and scan for vulnerabilities in the system and hosted applications [*weekly authenticated scans for operating systems (OS)-including databases, monthly unauthenticated scans for web application, annual authenticated scans for web applications*] and when new vulnerabilities potentially affecting the system are identified and reported;
b. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
    1. Enumerating platforms, software flaws, and improper configurations;
    2. Formatting checklists and test procedures; and
    3. Measuring vulnerability impact;
c. Analyze vulnerability scan reports and results from vulnerability monitoring;
d. Remediate legitimate vulnerabilities [
    (1) BOD Timelines
    (a) Within 14 days for vulnerabilities added to CISA's KEV Catalog with a CVE date post FY21.
    (b) Per the CISA KEV catalog date or GSA Standard timelines below, whichever is earlier, for vulnerabilities in the CISA KEV catalog with a CVE date in FY21 or earlier.
    (c) Within 15 days for Critical (Very High) vulnerabilities for Internet-accessible systems or services.
    (2) GSA Standard Timelines
    (a) Within 30 days for Critical (Very High) and High vulnerabilities.
    (b) Within 90 days for Moderate vulnerabilities.

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

(c) Within 120 days for Low vulnerabilities for Internet-accessible systems/services.]

in accordance with an organizational assessment of risk;

e. Share information obtained from the vulnerability monitoring process and control assessments with [*Information System Security Officers*] to help eliminate similar vulnerabilities in other systems; and
f. Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned

Control Enhancements:

(2) Vulnerability Monitoring and Scanning | Update Vulnerabilities to be Scanned – Update the system vulnerabilities to be scanned [*continuously – before each scan].*
(4) Vulnerability Monitoring and Scanning | Discoverable Information – Determine information about the system that is discoverable and take [*GSA S/SO recommended and GSA CISO and AO approved corrective actions]*
(5) Vulnerability Monitoring and Scanning | Privileged Access - Implement privileged access authorization to [*all information system components as applicable (e.g., OS, DB, Web App, etc.*] for [*all vulnerability scanning activities*].
(11) Vulnerability Monitoring and Scanning | Public Disclosure Program – Establish a public reporting channel for receiving reports of vulnerabilities in organizational systems and system components.

GSA Implementation Guidance:

CIO-IT Security-17-80 describes the weekly, monthly, and annual requirements for vulnerability scanning of GSA information systems and applications. It also describes an ad hoc process which can be used to scan for new vulnerabilities. CIO-IT Security-17-80 describes the scanning tools and techniques GSA uses to automate, as much as is possible, the scanning of GSA information systems and applications. It includes a description of the use of the Common Vulnerability Scoring System (CVSS) for assigning risks for tools that support CVSS. CIO-IT Security-17-80 assigns ISSOs the responsibility to evaluate and analyze scan reports and results in collaboration with information system personnel. GSA Order CIO 2100.1, this guide, and CIO-IT Security-17-80 all require remediation of:

- Critical/Very High vulnerabilities- for Internet-accessible IP addresses within 15 days, for all other assets within 30 days;
- High vulnerabilities within 30 days;
- Moderate vulnerabilities within 90 days

CIO-IT Security-17-80 describes how the different reports or dashboards are shared with ISSOs, ISSMs, and executives as necessary. Reports such as the Top 10 vulnerability summaries can be used to identify systemic issues across GSA.

As per RA-5, Enhancement (2), the scanning tools used by GSA's ISO Division are scheduled for auto-updates daily and update the tool configuration as necessary before running scans.

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

As per RA-5, Enhancement (4), GSA's ISO Division shares reports and dashboards with ISSOs who must coordinate with system personnel to take corrective actions to restrict discoverable information about systems as necessary.

As per RA-5, Enhancement (5), GSA FIPS 199 High Impact systems must collaborate with the ISO Division to implement privileged access to system assets in support of the vulnerability scanning capabilities described in CIO-IT Security-17-80.

As per RA-5, Enhancement (11), GSA's Vulnerability Disclosure Policy establishes GSA's public reporting channel for receiving reports of vulnerabilities in organizational systems and system components

Additional Contractor System Considerations: *Vendors/contractors must adhere to GSA policies and guides and comply with the control requirements.*

8.3.5 RA-7 Risk Response

Control: Respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance.

GSA Implementation Guidance:
ISSOs, System Owners, and system, network, and database administrators, will coordinate and perform remediation actions based upon the results of ongoing monitoring activities, assessment of risk, and outstanding items in the system's POA&M as described in Section 5.7.3 of this guide.

Additional Contractor System Considerations: *Vendors/contractors must adhere to GSA policies and guides and comply with the control requirements.*

8.3.6 RA-8 Privacy Impact Assessments

Control: Conduct privacy impact assessments for systems, programs, or other activities before:

a. Developing or procuring information technology that processes personally identifiable information; and;
b. Initiating a new collection of personally identifiable information that:
    1. Will be processed using information technology; and
    2. Includes personally identifiable information permitting the physical or virtual (online) contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, ten or more individuals, other than agencies, instrumentalities, or employees of the federal government.

Note: RA-8 is included in all FIPS 199 Baselines to ensure all systems complete a Privacy Threshold Assessment (PTA) to determine if a Privacy Impact Assessment (PIA) is required.

GSA Implementation Guidance:
GSA's Privacy Act Program website provides guidance on conducting Privacy Impact Assessments (PIAs), including links to CIO Order 1878.3, "Developing and Maintaining Privacy

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

Threshold Assessments (PTAs), PIAs, Privacy Act Notices, and System of Records Notices", and templates for PTAs and PIAs. The program and policy require developing PTAs and PIAs, when applicable, to identify PII before the development or acquisition of a new information system and to re-certify them annually.

Additional Contractor System Considerations: *Vendors/contractors must adhere to GSA policies and guides and comply with the control requirements.*

8.3.7 RA-9 Criticality Analysis

Control: Identify critical system components and functions by performing a criticality analysis for [*all systems as part of their Business Impact Analysis (BIA)*] at [*initial system design and development and throughout its lifecycle to ensure any criticality changes are identified*].

GSA Implementation Guidance:
GSA system owners, data owners, ISSOs, and ISSMs must identify the criticality of components as part of the Business Impact Analysis included in Contingency Planning activities. Throughout a system's lifecycle as changes to the system occur, they must be analyzed to determine if criticality of the system or its components has occurred.

Additional Contractor System Considerations: *Vendors/contractors must adhere to GSA policies and guides and comply with the control requirements.*

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

9 Additional NIST Controls Required by GSA

GSA requires certain controls be a part of a systems control set in accordance with the applicability listed in the following table.

Table 9-1: GSA Additional NIST Control Requirements

No.	Control No.	Control Name/Statement	Control Applicability
1	CA-2(1)	**Control Assessments | Independent Assessors** Employ independent assessors or assessment teams to conduct control assessments. **NOTE:** Independence is defined as when assessors do not: (i) have a mutual or conflicting interest with the organizations where the assessments are being conducted; (ii) assess their own work; (iii) act as management or employees of the organizations they are assessing; or (iv) place themselves in positions of advocacy for the organizations acquiring their services	In addition to the NIST requirement for FIPS 199 Moderate and High systems: • FIPS 199 Low external vendor/contractor systems
2	CA-8	**Penetration Testing** Conduct penetration testing [Assignment: organization-defined frequency] on [Assignment: organization-defined systems or system components]. The organization conducts penetration testing [*during A&A efforts and annually thereafter]* on *[all Internet accessible, FIPS 199 High impact, and High Value Asset (HVA) information systems*].	In addition to the NIST requirement for FIPS 199 High systems: • All Internet accessible systems • HVA information systems (See Section 8.1.7) • MiSaaS A&A systems
3	CA-8(1)	**Penetration Testing | Independent Penetration Agent or Team.** Employ an independent penetration testing agent or team to perform penetration testing on the system or system components. **NOTE:** Independence is waived for all annual testing (i.e., testing can be internally performed)	In addition to the NIST requirement for FIPS 199 High systems: • All Internet accessible systems • HVA information systems (See Section 8.1.7) • MiSaaS A&A systems
4	CM-2(2)	**Baseline Configuration | Automation Support for Accuracy / Currency** Maintain the currency, completeness, accuracy, and availability of the baseline configuration of the system using [*Assignment: organization-defined automated mechanisms*].	In addition to the NIST requirement for FIPS 199 Moderate and High systems: • Lightweight A&A systems • MiSaaS A&A systems • OA Program
5	CM-6(1)	**Configuration Settings | Automated Management, Application, and Verification** Manage, apply, and verify configuration settings for [*all operating systems*] using [*Assignment: organization-defined automated mechanisms*].	In addition to the NIST requirement for FIPS 199 High systems: • FIPS 199 Moderate systems • Lightweight A&A systems • MiSaaS A&A systems • OA Program

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

No.	Control No.	Control Name/Statement	Control Applicability
6	CM-8(2)	**System Component Inventory | Automated Maintenance** Maintain the currency, completeness, accuracy, and availability of the inventory of system components using [*Assignment: organization-defined automated mechanisms*].	In addition to the NIST requirement for FIPS 199 High systems: • FIPS 199 Moderate systems • Lightweight A&A systems • OA Program
7	CM-8(6)	**System Component Inventory | Assessed Configurations / Approved Deviations** Include assessed component configurations and any approved deviations to current deployed configurations in the system component inventory.	• FIPS 199 Moderate and High systems
8	CM-8(7)	**System Component Inventory | Centralize Repository** Provide a centralized repository for the inventory of system components.	• FIPS 199 Moderate and High systems
9	PE-8(3)	**Visitor Access Records | Limit Personally Identifiable Information Element** Limit personally identifiable information contained in visitor access records to the following elements identified in the privacy risk assessment: [individual visitor's name].	• FIPS 199 Moderate and High systems
10	PL-8	**Security and Privacy Architectures** a. Develop security and privacy architectures for the system that: 1. Describe the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of organizational information; 2. Describe the requirements and approach to be taken for processing personally identifiable information to minimize privacy risk to individuals; 3. Describe how the architectures are integrated into and support the enterprise architecture; and b. Review and update the architectures [*as necessary, and at least annually in conjunction with SSPP reviews/updates*] to reflect changes in the enterprise architecture; and c. Reflect planned architecture changes in security and privacy plans, Concept of Operations (CONOPS), criticality analysis, organizational procedures, and procurements and acquisitions.	In addition to the NIST requirement for FIPS 199 Moderate and High systems: • FIPS 199 Low systems • Lightweight A&A systems • OA Program
11	PL-9	**Central Management** Centrally manage [*common and hybrid security and privacy controls as identified in CIO-IT Security-18-90, Information Security Program Plan (ISPP)*].	• All systems

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

No.	Control No.	Control Name/Statement	Control Applicability
12	**RA-8**	Conduct privacy impact assessments for systems, programs, or other activities before: a. Developing or procuring information technology that processes personally identifiable information; and b. Initiating a new collection of personally identifiable information that: 1. Will be processed using information technology; and 2. Includes personally identifiable information permitting the physical or virtual (online) contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, ten or more individuals, other than agencies, instrumentalities, or employees of the federal government.	• All systems **Note:** RA-8 is included in all FIPS 199 Baselines to ensure all systems complete a Privacy Threshold Assessment (PTA) to determine if a Privacy Impact Assessment (PIA) is required. If the PTA determines a PIA is not required document RA-8 in the SSPP as "Implemented" and state in parts a and b "PTA completed, a PIA is not required."
13	**SA-3(2)**	**System Development Life Cycle | Use of Live or Operational Data** (a) Approve, document, and control the use of live data in preproduction environments for the system, system component, or system service; and (b) Protect preproduction environments for the system, system component, or system service at the same impact or classification level as any live data in use within the preproduction environments.	• All systems
16	**SC-8(1)**	**Transmission Confidentiality and Integrity | Cryptographic Protection** Implement cryptographic mechanisms to [prevent unauthorized disclosure of information and detect changes to information] during transmission.	In addition to the NIST requirement for FIPS 199 Moderate and High systems: • FIPS 199 Low systems • Lightweight A&A systems • MiSaaS A&A systems
17	**SC-28(1)**	**Protection of Information at Rest | Cryptographic Protection** Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on [*any system component, including databases (i.e., table, column, or field level) and applications*]: *[(1) Personally identifiable information; (2) Payment Card Industry data; (3) Authenticators, including but not limited to passwords, keys, and tokens; (4) business sensitive data as determined by the data owner and approved by the AO*]	In addition to the NIST requirement for FIPS 199 Moderate and High systems: • FIPS 199 Low systems • Lightweight A&A systems • MiSaaS A&A systems

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

No.	Control No.	Control Name/Statement	Control Applicability
18	**SI-2(3)**	**Flaw Remediation | Time to Remediate Flaws / Benchmarks for Corrective Actions** a. Measure the time between flaw identification and flaw remediation; and b. Establish the following benchmarks for taking corrective actions [(1) For Internet-accessible IP addresses (a) Any Critical (Very High) scan vulnerabilities must be remediated within 15 days. (b) Any High scan vulnerabilities must be remediated within 30 days. (c) Any Moderate scan vulnerabilities must be remediated within 90 days. (2) For all other assets (a) Any Critical (Very High) and High scan vulnerabilities must be remediated within 30 days. (b) Any Moderate scan vulnerabilities must be remediated within 90 days.] for taking corrective actions.	• FIPS 199 Moderate and High Systems • OA Program

10 Summary

Managing enterprise-level risk through a system life cycle perspective is a departure from the traditional view of security authorization as a static, procedural process. GSA has integrated EO 13800 and the NIST CSF throughout this guide by showing how they align with GSA's agency-wide use of the NIST RMF security authorization processes. The policies and procedures outlined in this guide provide an effective approach to system security authorization that is more dynamic and more capable of managing information system-related security risks across a diverse enterprise.

All GSA information systems must undergo a security control assessment and be authorized to operate according to their specific A&A process. GSA's standard A&A process requires A&A at least every three (3) years or whenever there is a significant change to the system's security posture in accordance with NIST SP 800-37.

GSA contractors and Federal employees should use this guide and the noted references prior to selecting and performing a security authorization process. Where there is a conflict between NIST guidance and GSA guidance, contact OCISO at ispcompliance@gsa.gov.

Note: In Appendix F, Table F-1, GSA has identified a list of Showstopper capabilities. Showstopper capabilities and associated NIST controls, if not fully implemented, may keep a system from receiving a full ATO.

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

Appendix A: CSF Function, Category, and Subcategory Definitions

The five CSF core function definitions are:

- **Identify (ID):** Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities. The activities in the Identify Function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Examples of outcome Categories within this Function include: Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy.
- **Protect: (PR):** Develop and implement appropriate safeguards to ensure delivery of critical services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Identity Management and Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.
- **Detect (DE):** Develop and implement appropriate activities to identify the occurrence of a cybersecurity event. The Detect Function enables timely discovery of cybersecurity events. Examples of outcome Categories within this Function include: Anomalies and Events; Security Continuous Monitoring; and Detection Processes.
- **Respond (RS):** Develop and implement appropriate activities to take action regarding a detected cybersecurity incident. The Respond Function supports the ability to contain the impact of a potential cybersecurity incident. Examples of outcome Categories within this Function include: Response Planning; Communications; Analysis; Mitigation; and Improvements.
- **Recover (RC):** Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident. Examples of outcome Categories within this Function include: Recovery Planning; Improvements; and Communications.

Table A-1 lists how NIST SP 800-37, Revision 2 maps the CSF functions listed above to the RMF steps. CSF category/subcategory identifiers are included in italics and parentheses after RMF tasks based on the task outcome tables in NIST SP 800-37. NIST identified some mappings to be to a Profile or to Implementation Tiers which are included in the table.

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

Table A-1: NIST CSF Functions Mapped to NIST SP 800-37 RMF Steps

CSF Function	Mapped RMF Steps
Identify	**Prepare Step:** Task P-1: Risk Management Roles (*ID.AM, ID.GV-2*) Task P-2: Risk Management Strategy (*ID.RM, ID.SC*) Task P-3: Risk Assessment – Organization (*ID.RM, ID.SC*) Task P-6: Impact-Level Prioritization (Optional) (*ID.AM-5*) Task P-7: Continuous Monitoring Strategy – Organization (*DE.CM, ID.SC-4*) Task P-8: Mission or Business Focus (*Profile; Implementation Tiers, ID.BE*) Task P-9: System Stakeholders (*ID.AM; ID.BE*) Task P-10: Asset Identification (*ID.AM*) Task P-11: Authorization Boundary (*N/A*) Task P-12: Information Types (*ID.AM-5*) Task P-13: Information Life Cycle (*ID.AM-3, ID.AM-4*) Task P-14: Risk Assessment – System (*ID.RA, ID.SC-2*) Task P-15 Requirements Definition (*ID.GV, PR.IP*) Task P-16: Enterprise Architecture (*N/A*) Task P-17: Requirements Allocation (*ID.GV*) Task P-18: System Registration (*ID.GV*) **Categorize Step:** Task C-1: System Description (*Profile*) Task C-2: Security Categorization (*ID.AM-1, ID.AM-2, ID.AM-3, ID.AM-4, ID.AM-5, Profile*) Task C-3: Security Categorization Review and Approval (*N/A*) **Select Step:** Task S-1: Control Selection (*Profile*) Task S-2: Control Tailoring (*Profile*) Task S-3: Control Allocation (*Profile, PR.IP*) Task S-4: Documentation of Planned Control Implementations (*Profile*) Task S-5: Continuous Monitoring Strategy – System (*ID.GV, DE.CM*) **Assess Step:** Task A-6: Plan of Action and Milestones (*ID.RA-6*) **Authorize Step:** Task R-3: Risk Response (*ID.RA-6*) Task R-5: Authorization Reporting (*N/A*) **Monitor Step:** Task M-1: System and Environment Changes (*DE.CM, ID.GV*) Task M-2: Ongoing Assessments (*ID.SC-4*) Task M-5: Security and Privacy Reporting (*N/A*)
Protect	**Prepare Step:** Task P-15 Requirements Definition (*ID.GV, PR.IP*) **Select Step:** Task S-1: Control Selection (*Profile*) Task S-2: Control Tailoring (*Profile*) Task S-3: Control Allocation (*Profile, PR.IP*) Task S-4: Documentation of Planned Control Implementations (*Profile*) **Implement Step:** Task I-1: Control Implementation (*PR.IP-1, PR.IP-2*) Task I-2: Update Control Implementation Information (*PR.IP-1, Profile*) **Authorize Step:** Task R-5: Authorization Reporting (*N/A*) **Monitor Step:**

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

CSF Function	Mapped RMF Steps
	Task M-5: Security and Privacy Reporting (*N/A*)
Detect	**Prepare Step:** Task P-7 Continuous Monitoring Strategy – Organization Task P-15 Requirements Definition (*ID.GV, PR.IP*) **Select Step:** Task S-1: Control Selection (*Profile*) Task S-2: Control Tailoring (*Profile*) Task S-4: Documentation of Planned Control Implementations (*Profile*) Task S-5: Continuous Monitoring Strategy – System (*ID.GV, DE.CM*) **Authorize Step:** Task R-5: Authorization Reporting (*N/A*) **Monitor Step:** Task M-1: System and Environment Changes (*DE.CM, ID.GV*) Task M-5: Security and Privacy Reporting (*N/A*)
Respond	**Prepare Step:** Task P-15 Requirements Definition (*ID.GV, PR.IP*) **Select Step:** Task S-1: Control Selection (*Profile*) Task S-2: Control Tailoring (*Profile*) Task S-4: Documentation of Planned Control Implementations (*Profile*) **Authorize Step:** Task R-5: Authorization Reporting (*N/A*) **Monitor Step:** Task M-3: Ongoing Risk Response (*RS.AN*) Task M-4: Authorization Package Updates (*RS.IM*) Task M-5: Security and Privacy Reporting (*N/A*)
Recover	**Prepare Step:** Task P-15 Requirements Definition (*ID.GV, PR.IP*) **Select Step:** Task S-1: Control Selection Task S-2: Control Tailoring Task S-4: Documentation of Planned Control Implementations **Authorize Step:** Task R-5: Authorization Reporting **Monitor Step:** Task M-5: Security and Privacy Reporting (*N/A*)
N/A	**Prepare Step:** Task P-4: Organizationally – Tailored Control Baselines and Cybersecurity Framework Profiles (Optional) (*Profile*) Task P-5: Common Control Identification (*N/A*) **Select Step:** Task S-6: Plan Review and Approval (*N/A*) **Assess Step:** Task A-1: Assessor Selection (*N/A*) Task A-2: Assessment Plan (*N/A*) Task A-3: Control Assessments (*N/A*) Task A-4: Assessment Reports (*N/A*) Task A-5: Remediation Actions (*Profile*) **Authorize Step:** Task R-1: Authorization Package Task R-2: Risk Analysis and Determination

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

CSF Function	Mapped RMF Steps
	Task R-4: Authorization Decision **Monitor Step:** Task M-6: Ongoing Authorization (*N/A*) Task M-7: System Disposal (*N/A*)

Table A-2, CSF Category/Subcategory Definitions, provides the definitions for CSF Categories and Subcategory Unique Identifiers. GSA is aligned with the CSF via the implementation of the NIST SP 800-53 controls which address the subcategory requirements. NIST CSF Version 1.1 provides an informative (i.e., not establishing a normative standard) listing of NIST SP 800-53 controls to the subcategories. Rows highlighted in yellow in the Table A-2 depict CSF Categories/Subcategories that NIST indicates in the CSF are associated with the CA, PL, and RA controls in Section 8.

Table A-2: CSF Category/Subcategory Definitions

Category/Subcategory Unique Identifiers	Definition
Asset Management (ID.AM)	The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.
ID.AM-1	Physical devices and systems within the organization are inventoried
ID.AM-2	Software platforms and applications within the organization are inventoried
ID.AM-3	Organizational communication and data flows are mapped
ID.AM-4	External information systems are catalogued
ID.AM-5	Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value
ID.AM-6	Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established
Business Environment (ID.BE)	The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.
ID.BE-1	The organization's role in the supply chain is identified and communicated
ID.BE-2	The organization's place in critical infrastructure and its industry sector is identified and communicated
ID.BE-3	Priorities for organizational mission, objectives, and activities are established and communicated
ID.BE-4:	Dependencies and critical functions for delivery of critical services are established
ID.BE-5	Resilience requirements to support delivery of critical services are established for all operating states (e.g., under duress/attack, during recovery, normal operations)
Governance (ID.GV)	The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.
ID.GV-1	Organizational cybersecurity policy is established and communicated
ID.GV-2	Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners
ID.GV-3	Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed
ID.GV-4	Governance and risk management processes address cybersecurity risks

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

Category/Subcategory Unique Identifiers	Definition
Risk Assessment (ID.RA)	The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.
ID.RA-1	Asset vulnerabilities are identified and documented
ID.RA-2	Cyber threat intelligence is received from information sharing forums and sources
ID.RA-3	Threats, both internal and external, are identified and documented
ID.RA-4	Potential business impacts and likelihoods are identified
ID.RA-5	Threats, vulnerabilities, likelihoods, and impacts are used to determine risk
ID.RA-6	Risk responses are identified and prioritized
Risk Management Strategy (ID.RM)	The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.
ID.RM-1	Risk management processes are established, managed, and agreed to by organizational stakeholders
ID.RM-2	Organizational risk tolerance is determined and clearly expressed
ID.RM-3	The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis
Supply Chain Risk Management (ID.SC)	The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.
ID.SC-1	Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders
ID.SC-2	Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process
ID.SC-3	Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan
ID.SC-4	Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations
ID.SC-5	Response and recovery planning and testing are conducted with suppliers and third-party providers
Identity Management, Authentication and Access Control (PR.AC)	Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.
PR.AC-1	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes
PR.AC-2	Physical access to assets is managed and protected
PR.AC-3	Remote access is managed
PR.AC-4	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties
PR.AC-5	Network integrity is protected (e.g., network segregation, network segmentation)
PR.AC-6	Identities are proofed and bound to credentials and asserted in interactions
PR.AC-7	Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

Category/Subcategory Unique Identifiers	Definition
Awareness and Training (PR.AT)	The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.
PR.AT-1	All users are informed and trained
PR.AT-2	Privileged users understand roles and responsibilities
PR.AT-3	Third-party stakeholders (e.g., suppliers, customers, partners) understand roles and responsibilities
PR.AT-4	Senior executives understand roles and responsibilities
PR.AT-5	Physical and information security personnel understand roles and responsibilities
Data Security (PR.DS)	Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
PR.DS-1	Data-at-rest is protected
PR.DS-2	Data-in-transit is protected
PR.DS-3	Assets are formally managed throughout removal, transfers, and disposition
PR.DS-4	Adequate capacity to ensure availability is maintained
PR.DS-5	Protections against data leaks are implemented
PR.DS-6	Integrity checking mechanisms are used to verify software, firmware, and information integrity
PR.DS-7	The development and testing environment(s) are separate from the production environment
PR.DS-8	Integrity checking mechanisms are used to verify hardware integrity
Information Protection Processes and Procedures (PR.IP)	Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.
PR.IP-1	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g., concept of least functionality)
PR.IP-2	A System Development Life Cycle to manage systems is implemented
PR.IP-3	Configuration change control processes are in place
PR.IP-4	Backups of information are conducted, maintained, and tested
PR.IP-5	Policy and regulations regarding the physical operating environment for organizational assets are met
PR.IP-6	Data is destroyed according to policy
PR.IP-7	Protection processes are improved
PR.IP-8	Effectiveness of protection technologies is shared
PR.IP-9	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed
PR.IP-10	Response and recovery plans are tested
PR.IP-11	Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)
PR.IP-12	A vulnerability management plan is developed and implemented
Maintenance (PR.MA)	Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.
PR.MA-1	Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools
PR.MA-2	Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

Category/Subcategory Unique Identifiers	Definition
Protective Technology (PR.PT)	Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.
PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy
PR.PT-2	Removable media is protected and its use restricted according to policy
PR.PT-3	The principle of least functionality is incorporated by configuring systems to provide only essential capabilities
PR.PT-4	Communications and control networks are protected
PR.PT-5	Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations
Anomalies and Events (DE.AE)	Anomalous activity is detected and the potential impact of events is understood.
DE.AE-1	A baseline of network operations and expected data flows for users and systems is established and managed
DE.AE-2	Detected events are analyzed to understand attack targets and methods
DE.AE-3	Event data are collected and correlated from multiple sources and sensors
DE.AE-4	Impact of events is determined
DE.AE-5	Incident alert thresholds are established
Security Continuous Monitoring (DE.CM)	The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.
DE.CM-1	The network is monitored to detect potential cybersecurity events
DE.CM-2	The physical environment is monitored to detect potential cybersecurity events
DE.CM-3	Personnel activity is monitored to detect potential cybersecurity events
DE.CM-4	Malicious code is detected
DE.CM-5	Unauthorized mobile code is detected
DE.CM-6	External service provider activity is monitored to detect potential cybersecurity events
DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed
DE.CM-8	Vulnerability scans are performed
Detection Processes (DE.DP)	Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.
DE.DP-1	Roles and responsibilities for detection are well defined to ensure accountability
DE.DP-2	Detection activities comply with all applicable requirements
DE.DP-3	Detection processes are tested
DE.DP-4	Event detection information is communicated
DE.DP-5	Detection processes are continuously improved
Response Planning (RS.RP)	Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity events.
RS.RP-1:	Response plan is executed during or after an incident
Communications (RS.CO)	Response activities are coordinated with internal and external stakeholders (e.g., external support from law enforcement agencies).
RS.CO-1	Personnel know their roles and order of operations when a response is needed
RS.CO-2	Incidents are reported consistent with established criteria
RS.CO-3	Information is shared consistent with response plans
RS.CO-4	Coordination with stakeholders occurs consistent with response plans
RS.CO-5	Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

Category/Subcategory Unique Identifiers	Definition
Analysis (RS.AN)	Analysis is conducted to ensure effective response and support recovery activities.
RS.AN-1	Notifications from detection systems are investigated
RS.AN-2	The impact of the incident is understood
RS.AN-3	Forensics are performed
RS.AN-4	Incidents are categorized consistent with response plans
RS.AN-5	Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g., internal testing, security bulletins, or security researchers)
Mitigation (RS.MI)	Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.
RS.MI-1	Incidents are contained
RS.MI-2	Incidents are mitigated
RS.MI-3	Newly identified vulnerabilities are mitigated or documented as accepted risks
Improvements (RS.IM)	Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.
RS.IM-1	Response plans incorporate lessons learned
RS.IM-2	Response strategies are updated
Recovery Planning (RC.RP)	Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.
RC.RP-1	Recovery plan is executed during or after a cybersecurity incident
Improvements (RC.IM)	Recovery planning and processes are improved by incorporating lessons learned into future activities.
RC.IM-1	Recovery plans incorporate lessons learned
RC.IM-2	Recovery strategies are updated
Communications (RC.CO)	Restoration activities are coordinated with internal and external parties (e.g., coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).
RC.CO-1	Public relations are managed
RC.CO-2	Reputation after an event is repaired
RC.CO-3	Recovery activities are communicated to internal and external stakeholders as well as executive and management teams

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

Appendix B: Consolidated List of Guidance, Policies, Procedures, Templates

Federal Regulations/Guidance:

- DHS Cybersecurity Directives
- EO 13800, "Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure"
- FIPS 140-2, "Security Requirements for Cryptographic Modules"
- FIPS 140-3, "Security Requirements for Cryptographic Modules"
- FIPS 199, "Standards for Security Categorization of Federal Information and Information Systems"
- FIPS 200, "Minimum Security Requirements for Federal Information and Information Systems"
- NIST CSF, "Framework for Improving Critical Infrastructure Cybersecurity"
- NIST SP 800-18, Revision 1, "Guide for Developing Security Plans for Federal Information Systems"
- NIST SP 800-30 Revision 1, "Guide for Conducting Risk Assessments"
- NIST SP 800-37, Revision 2, "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy"
- NIST SP 800-47, Revision 1, "Managing the Security of Information Exchanges"
- NIST SP 800-53, Revision 5, "Security and Privacy Controls for Information Systems and Organizations"
- NIST SP 800-53B, "Control Baselines for Information Systems and Organizations"
- NIST SP 800-60, Volume I, Revision 1, "Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories"
- NIST SP 800-60, Volume II, Revision 1, "Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories"
- NIST SP 800-171, Revision 2, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations"
- Public Law 113-283, "Federal Information Security Modernization Act of 2014"

GSA Guidance:

The GSA policies listed below are available on the GSA.gov Directives Library page.

- GSA Order CIO 2100.1, "GSA Information Technology (IT) Security Policy"
- GSA Order CIO 1878.3, "Developing and Maintaining Privacy Threshold Assessments (PTAs), PIAs, Privacy Act Notices, and System of Records Notices"
- GSA Order CIO 2140.4, "Information Technology (IT) Solutions Life Cycle (SLC) Policy"
- GSA Order CIO 2183.1, "Enterprise Identity, Credential, and Access Management (ICAM) Policy"

The GSA CIO-IT Security Procedural Guides listed below are available on the GSA.gov IT Security Procedural Guides page with the exception of CIO-IT Security-18-90 which is restricted. It is available on the internal GSA InSite IT Security Procedural Guides page.

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

- GSA CIO-IT Security-01-05, "Configuration Management (CM)"
- GSA CIO-IT Security-06-30, "Managing Enterprise Cybersecurity Risk"
- GSA CIO-IT Security-06-32, "Media Protection (MP)"
- GSA CIO-IT Security-07-35, "Web Application Security"
- GSA CIO-IT Security-08-39, "IT Security Program Management Implementation Plan"
- GSA CIO-IT Security-09-44, "Plan of Action and Milestones (POA&M)"
- GSA CIO-IT Security-09-48, "Security and Privacy Requirements for IT Acquisition Efforts"
- GSA CIO-IT Security-11-51, "Conducting Penetration Test Exercises"
- GSA CIO-IT Security-11-62, "Salesforce Platform Security Implementation"
- GSA CIO-IT Security-12-66, "Information Security Continuous Monitoring (ISCM) Strategy & Ongoing Authorization (OA) Program"
- GSA CIO-IT Security-14-68, "Lightweight Security Authorization Process"
- GSA CIO-IT Security-16-75, "Low Impact Software as a Service (LiSaaS) Solutions Authorization Process"
- GSA CIO-IT Security-18-88, "Moderate Impact Software as a Service (MiSaaS) Security Authorization Process"
- GSA CIO-IT Security-18-90, "Information Security Program Plan (ISPP)"
- GSA CIO-IT Security-18-91, "Risk Management Strategy (RMS)"
- GSA CIO-IT Security-19-95, "Security Engineering Architecture Reviews"
- GSA CIO-IT Security-19-101, "External Information System Monitoring"
- GSA CIO-IT Security-21-112, "Protecting Controlled Unclassified Information (CUI) in Nonfederal Systems and Organizations Process"—under development
- GSA CIO-IT Security-21-114, "Clean Authorizations to Operate (ATOs) at GSA"—under development

The GSA CIO-IT Security Forms (document templates) listed below are available on the IT Security Forms page.

- FIPS 199 Security Categorization Template
- Digital Identity Acceptance Statement
- GSA Control Tailoring Workbook
- FIPS 199 Low, Moderate, and Control Implementation Summaries
- Low, Moderate, and High System Security and Privacy Plan Templates
- Low, Moderate, and High NIST 800-53 Revision 5 Test Cases
- Security Assessment Plan (SAP) Template
- Security Assessment Report (SAR) Template
- ATO Letter Template
- Certification Letter Template
- Low, Moderate, and High Information System Contingency Plan Templates
- Information System Contingency Plan Test Plan Template
- Information System Contingency Plan Test Report Template
- Interconnection Security Agreement Template
- MiSaaS Test Case Workbook
- MiSaaS SSPP Template

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

- Penetration Test Exercise Templates:
  - RoE Kickoff Presentation Template
  - Assessment Penetration Test Rules of Engagement Template
  - Penetration Test Report Template
  - OWASP v4 Testing Checklist
- POA&M Share Drive User Access Request Form
- ISCM Ongoing Authorization Letter Template
- Salesforce Platform Documentation Templates
- Transfer Notification Template
- Disposal Notification Template

Privacy Threshold Analysis/Privacy Impact Assessment information is available on GSA's IT Privacy page.

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

Appendix C: A&A Process Package Document Lists/Links

This Appendix contains a listing of the A&A Package documentation requirements for each of the A&A processes described in this guide, document templates are available on the IT Security Forms page, procedural guides are available on the IT Security Procedural Guides page with the exception of CIO-IT Security-18-90 which is restricted. It is available on the internal GSA InSite IT Security Procedural Guides page. Search for the title of the template/form/document listed to obtain its current version. Additional documents may be required of contractor systems as identified in CIO-IT Security-19-101.

Standard A&A Process
Documents
System Security and Privacy Plan (Low, Moderate, High) Appendix A - Acronyms, Terms, and Definitions Appendix B - References Appendix C - Hosted Subsystems (if applicable) Other Appendices, as necessary Attachment 1: Privacy Threshold Analysis / Privacy Impact Assessment Attachment 2: FIPS 199 Security Categorization Attachment 3: Digital Identity Acceptance Statement Attachment 4: Interconnection Security Agreement Attachment 5: Control Tailoring Workbook (CTW) Attachment 6: Control Implementation Summary Table (Low, Moderate, High) Attachment 7: Contingency Plan (Low, Moderate, High) Attachment 8: Contingency Plan Test Report Attachment 9: Incident Response Plan Attachment 10: Incident Response Plan Test Report Attachment 11: Configuration Management Plan Attachment 12: Continuous Monitoring Plan (if applicable) Attachment 13: Code Review Report (if applicable) Other Attachments, as necessary
Security Assessment Report (Results from the Security Assessment Plan) Appendix A - Acronyms, Terms, and Definitions Appendix B - NIST 800-53 Test Cases Appendix C - Operating System Scanning Results Appendix D - Database Application Scanning Results Appendix E - Web Application Scanning Results Other Appendices, as necessary Attachment 1: Penetration Test Report Other Attachments, as necessary
Plan of Action and Milestones (POA&M)
Certification Memorandum
ATO Letter

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

Lightweight Security Authorization Process
Documents
System Security and Privacy Plan (with appendices/attachments) Appendix A - References Attachment 1: Privacy Threshold Analysis/Privacy Impact Assessment Attachment 2: FIPS 199 Security Categorization Attachment 3: Digital Identity Acceptance Statement Attachment 4: Code Review Report Attachment 5: Penetration Test Results (if applicable) Attachment 6: Vulnerability Scan Results Security Assessment Report (with appendices/attachments) Appendix A - Acronyms Attachments: Additional Supporting Documents (as necessary, see note below) **Note**: Systems receiving a 1-year LATO or 3-year full ATO would have a SAR with Attachments 4-5 of the SSPP typically included in the SAR instead of the SSPP.
POA&M
CRM - Please contact your ISSM to receive the vendor's current CRM for your system.
Certification Memorandum
ATO Letter

Security Reviews for Low Impact Software as a Service Solutions Process
Documents
LiSaaS Solution Review Checklist
Checklist Supporting Artifacts
LiSaaS Solution Profile (only if Very Low/Negligible Risk)
Attestation Letter (if applicable)
ATO Letter

GSA Agency FedRAMP Process
Documents
Note: The FedRAMP A&A documentation templates are available on the FedRAMP website under Documents and Templates. Please visit that website to get the current templates.
System Security Plan
Security Assessment Plan
NIST 800-53 Revision 4 Test Cases
Security Assessment Report
(Vendors) Users Guide)
Control Implementation Summary
POA&M
FIPS 199 Categorization
e-Authentication Level
Rules of Behavior
(Vendors) Configuration Management Plan

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

GSA Agency FedRAMP Process
(Vendors) Information System Security Policies
IT Contingency Plan
(Vendors) Incident Response Plan
Privacy Threshold Analysis and PIA

Moderate Impact Software as a Service (MiSaaS) Security Authorization Process
Documents
System Security and Privacy Plan MiSaaS SSPP Template
Security Assessment Report Security Assessment Report (including, as applicable) • MiSaaS Test Workbook • Vulnerability Scan Data • Penetration Test Report
POA&M
CRM - Please contact your ISSM to receive the vendor's current CRM for your system.
Certification Memorandum
ATO Letter

GSA Subsystem A&A Process
Documents
FIPS 199 Low Subsystem
See Lightweight Security Authorization Process Documentation)
FIPS 199 Moderate Subsystem
System Security and Privacy Plan (Low, Moderate, High) (only hybrid and system specific controls)
NIST 800-53 Test Cases (only hybrid and system specific controls)
Security Assessment Report (only hybrid and system specific controls)

GSA Ongoing Authorization Program
Documents
OATO Package • OA Checklist (with supporting artifacts) • Onboarding Assessment Report
OATO Letter

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

GSA Leveraged FedRAMP XaaS Solution Process
Documents
CRM System Security Plan, including: Attachment 1: Privacy Threshold Analysis/Privacy Impact Assessment (if applicable) Attachment 2: FIPS 199 Security Categorization Attachment 3: Digital Identity Acceptance Statement Other Attachments, as necessary
CRM Evidentiary supporting artifacts, as necessary
Assessment Artifacts FIPS 199 Low: Self-attestation statement Assessment test cases, automated tool results, etc.
Certification Memorandum
ATO Letter

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

Appendix D: GSA Defined Cloud Controls

GSA's Control Tailoring Workbook contains a Sheet (Tab) with GSA's assignment parameters for GSA Cloud Control Settings for FIPS 199 Low and Moderate baselines. These parameter settings must be used by CSPs working with GSA pursuing an authorization under the FedRAMP program. CSPs must also address the other controls in FedRAMP's baselines using FedRAMP's assignment parameters.

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

Appendix E: Scanning Frequency By A&A Process

Scanning/testing frequency by component type and A&A process are listed in the 06-30 Scanning Parameter Spreadsheet.

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

Appendix F: Showstopper Capabilities and Associated Controls

Table F-1 lists the Showstopper Capabilities and associated NIST SP 800-53 controls that GSA has identified that, if not fully compliant, will keep a system from receiving a full ATO.

Table F-1: GSA Showstopper Capabilities/Controls

#	Showstopper Description	Control Reference
1	Multi-Factor Authentication (MFA) for Privileged & User-level access: All systems shall utilize a GSA-approved multi-factor authentication mechanism for both privileged and non-privileged user authentication. Further, systems leveraging certificate-based authentication shall not be downgraded to only username and password authentication. Per NIST 800-63B, "Digital Identity Guidelines, Authentication and Lifecycle Management," MFA methods involving the sending of PINS/passwords via email is prohibited and on public networks via SMS is restricted. Sending PINS/passwords to registered telephone numbers on GFE is allowed based on a risk analysis. MFA methods shall favor approaches that do not expose PINS/passwords to intercept risk including but not limited to HOTP, TOTP, SAML/OIDC, PIV, FIDO/WebAuthn. If an assessment identifies MFA has not been implemented, per policy requirements, then the system will not be approved for a 3-year ATO or OA, until MFA is implemented.	IA-2 (1) Identification and Authentication (Organizational Users) | Multifactor Authentication to Privileged Accounts IA-2 (2) Identification and Authentication (Organizational Users) | Multifactor Authentication to Non-Privileged Accounts
2	Critical and High vulnerabilities: GSA requires ongoing remediation actions including patching, updating, and upgrading out of date components, addressing known vulnerabilities, completing POA&Ms, maintaining secure configurations of components. If an assessment identifies ongoing remediation actions are not being addressed, then the system will not be approved for a 3-year ATO or OA, until the associated risks are mitigated.	SI-2 Flaw Remediation
3	Remote Code Execution (RCE) Vulnerabilities: RCE vulnerabilities can be exploited if user input is injected into a File or a String and executed (evaluated) by the programming language's parser. RCE vulnerabilities must be remediated, regardless of the RCE system impact level identified. If an information system is identified with an RCE vulnerability during an assessment, then the system will not be approved for a 3-year ATO or OA, until the risk is mitigated.	SI-2 Flaw Remediation
4	EOL Software: The continued usage of End of Life (EOL) Software requires a risk evaluation to be performed by the OCISO. An EOL Software usage justification to include POA&M tracking requirements or an approved Acceptance of Risk (AOR), are the possible documentation outcome requirements of the risk evaluation. If an assessment identifies EOL software usage has not been properly evaluated and documented, then the system will not be approved for a 3-year ATO or OA,	SA-22 Unsupported System Components

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

#	Showstopper Description	Control Reference
	until completed.	
5	System Architecture has been reviewed and approved by ISE: CIO-IT Security-19-95, "Security Engineering Architectural Reviews" identifies the OCISO Security Engineering (ISE) system evaluation requirements. If an assessment identifies an ISE system review has not been completed for the system, then the system will not be approved for a 3-year ATO or OA, until one is completed.	PL-8 Security and Privacy Architecture SA-8 Security and Privacy Engineering Principles
6	Integration with GSA's Security Stack (Internal Systems): System integration includes; • Sending logs to GSA's central Enterprise Logging Platform (ELP) to support information system monitoring. • Using GSA's configuration setting monitoring tools (BigFix, MasS360). • Installing GSA's tool for whitelisting/blacklisting and restricting user installation of software (Bit9). • Using GSA's scanning tools to identify vulnerabilities (e.g., Tenable Security Center (TSC), NetSparker). • Using GSA's antivirus and malicious code protection tools (e.g., Cylance AV, FireEye). • Using GSA's inventory management tools (e.g., BigFix, ServiceNow, Forescout/SecureConnector, MaaS260) to monitor assets. **Note:** Tools referenced above relate to GSA's internal infrastructure and systems those tools can be integrated with; GSA cloud environments (e.g., FCS, GRACE) may vary. If an assessment identifies the system has not been integrated with the GSA Security Stack (based upon the specific system requirements), then the system will not be approved for a 3-year ATO or OA, until the deployment requirements have been completed.	Additional details on GSA's security stack can be found in this Google Sheet. GSA ISCM Enterprise Security Management Tools
7	Encryption of Sensitive Data (i.e., PII, PCI, Authenticators): **Systems that process Personally Identifiable Information (PII), Payment Card Industry (PCI) data, Authenticators (e.g., passwords, tokens, keys, certificates, hashes, etc.), and other sensitive data as determined by the AO, shall encrypt that data everywhere (i.e., at file level, database level, at rest, and in transit. For databases, encryption of the whole database, table, column, or field levels is acceptable, as appropriate. Other methods including, but not limited to, application encryption or tokenization is also acceptable. For web services connections, implement end to end encryption terminating the connection at the web server; connections terminated at a load balancer shall employ re-encryption techniques to ensure end to end encryption.** If an assessment identifies the system has not addressed data encryption based upon the specific system's data protection requirements, then the system will not be approved for a 3-year ATO or OA, until the deployment requirements have been completed.	SC-8 Transmission Confidentiality and Integrity SC-8(1) Transmission Confidentiality and Integrity | Cryptographic Protection SC-28 Protection of Information at Rest SC-28 (1) Protection of Information at Rest | Cryptographic Protection

DocuSign Envelope ID: 332208CA-6E8E-4C81-9282-256CFB3003ED

#	Showstopper Description	Control Reference
	Encryption algorithms and modules shall be FIPS 140-2/140-3[5], "Security Requirements for Cryptographic Modules," validated. • Digital signature encryption algorithms • Block cypher encryption algorithms • Secure hashing algorithms For web services connections, implement end to end encryption terminating the connection at the web server; connections terminated at a load balancer shall employ re-encryption techniques to ensure end to end encryption. Internet accessible Websites shall implement HTTPS Only with HTTP Strict Transport Security (HSTS), have no weak ciphers, have no weak protocols, and preload .gov domains. (see BOD 18-01, Enhance Email and Web Security). SSL/TLS implementations shall align with GSA IT Security Procedural Guide 14-69, "SSL/TLS Implementation."	
8	Compliance with CISA ED/BOD: Log4J must be fully upgraded to a secure version (currently 2.16) per ED 22-02. Per BOD 22-01, the system must not have any vulnerabilities identified in the CISA KEV Catalog. If an assessment identifies a system does not have Log4J fully upgraded or has vulnerabilities form the DHS CISA KEV Catalog, then the system will not be approved for an ATO.	SI-2 Flaw Remediation

[5] NIST has issued FIPS 140-3, FIPS 140-2 modules are still being validated and will be accepted through September 22, 2026. For additional information see the NIST cryptographic module validation program web page.

GENERAL SERVICES ADMINISTRATION
Washington, DC 20405

CIO 2100.1N
9/21/2022

GSA ORDER

SUBJECT: GSA Information Technology (IT) Security Policy

1. Purpose. This Chief Information Officer (CIO) Order establishes the General Services Administration (GSA) IT Security Policy.

2. Cancellation. This Order cancels and supersedes CIO 2100.1M, GSA Information Technology (IT) Security Policy, dated March 26, 2021.

3. Explanation of Changes. This Order provides updates for consistency with Federal requirements and program instruction implementation. Changes include:

a. Added references to recent Executive Orders and Office of Management and Budget (OMB) Memoranda;
b. Added Section 14 on zero trust architecture;
c. Added critical software inventory policy statements at Chapter 3, Section 1, part c;
d. Added policy statement at Chapter 4, Section 6, part b, regarding the need to provide logs upon request to the Department of Homeland Security (DHS), Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) consistent with applicable laws;
e. Updated Supply Chain Risk Management section;
f. Updated sections on multifactor authentication and passwords;
g. Updated Required Warning Banner;
h. Added specific requirements on encryption of data at rest and in transit; and
i. Added restrictions on the use of organization-controlled portable storage devices usage on external systems.

4. Applicability.

a. This IT Security Policy applies to all:

(1) GSA Federal employees, contractors, and vendors of GSA, who manage, maintain, operate, or protect GSA systems or data;

(2) IT systems owned and operated by or on the behalf of any of the GSA Service and Staff Offices (SSOs), including Regional Offices; and

(3) GSA or Federal data contained on or processed by IT systems owned and operated by or on the behalf of any of the GSA SSOs, including Regional Offices.

b. Except for Chapter 2, section 21, this policy applies to the Office of Inspector General (OIG) only to the extent that the OIG determines it is consistent with the OIG's independent authority under the IG Act and it does not conflict with other OIG policies or the OIG mission.

c. This policy applies to the Civilian Board of Contract Appeals (CBCA) only to the extent that the CBCA determines it is consistent with the CBCA's independent authority under the Contract Disputes Act and other authorities and it does not conflict with the CBCA's policies or the CBCA mission.

5. Signature.

/S/_____
DAVID SHIVE
Chief Information Officer
Office of GSA IT

Table of Contents

CHAPTER 1: THE GSA INFORMATION TECHNOLOGY SECURITY PROGRAM 5
CHAPTER 2: SECURITY ROLES AND RESPONSIBILITIES 15
CHAPTER 3: POLICY FOR IDENTIFY FUNCTION 39
CHAPTER 4: POLICY FOR PROTECT FUNCTION 46
CHAPTER 5: POLICY FOR DETECT FUNCTION 71
CHAPTER 6: POLICY FOR RESPOND FUNCTION 75
CHAPTER 7: POLICY FOR RECOVER FUNCTION 78
Appendix A: CSF CATEGORIES/SUBCATEGORIES 79

CHAPTER 1: THE GSA INFORMATION TECHNOLOGY SECURITY PROGRAM

1. Introduction. The purpose of this Order is to document and set forth GSA's IT Security Policy. This IT Security Policy establishes controls required to comply with Federal laws and regulations (including CISA Cybersecurity Directives) and thus facilitates adequate protection of GSA IT resources.

2. Objectives. IT Security Policy objectives will enable GSA to meet its mission and business objectives by implementing systems with due consideration of IT related risks to GSA, its partners, and customers. The security objectives for system resources are to provide assurance of confidentiality, integrity, availability, accountability, and resilience by employing security controls to manage cybersecurity risk in accordance with (IAW) Executive Order (EO) 13800 and the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). An important component of risk-based management is to integrate technical and non-technical security mechanisms and techniques into a system to reflect sound risk management practices. All incorporated security mechanisms must be well founded, configured to perform in the most effective manner, and add value to GSA's IT-related investments. This risk-based approach will enable the GSA IT Security Program to meet its goals by better securing IT systems; providing management the information necessary to justify IT Security expenditures; and assisting GSA in authorizing IT systems for operation.

GSA IT security objectives include the following:

a. Confidentiality. Preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and Controlled Unclassified Information (CUI). Private or confidential information is not disclosed to unauthorized individuals while at rest, during processing, or in transit.

b. Integrity. Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity. Safeguards must ensure information retains its content integrity. Unauthorized personnel must not be able to create, alter, copy, or delete data processed, stored, or handled by the system.

c. Availability. Ensuring timely and reliable access to and use of information. The system works promptly, and service is not denied to authorized users. The system must be ready for use by authorized users when needed to perform their duties.

d. Accountability. Accountability must be to the individual level. Only personnel with proper authorization and need-to-know must be allowed access to data processed, handled, or stored on IT system components.

e. Assurance. Measure of confidence that the security features, practices, procedures, and architecture of an information system accurately mediates and enforces the security policy. This assurance (i.e., confidence that the other four security

objectives have been met), is provided through assessment and monitoring of security mechanisms and controls.

f. Resilience. The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.

This Order supports GSA's IT Security Program objectives by:

- Identifying roles and assigning responsibilities in support of GSA's IT Security Program;
- Defining comprehensive and integrated security requirements that are necessary to protect CUI (e.g., Personally Identifiable Information [PII], building drawings, proprietary data) and allow GSA IT systems to operate within an acceptable level of residual risk;
- Supporting GSA's objective to ensure that all outsourced cloud services are from Federal Risk and Authorization Management Program (FedRAMP) authorized (or in the process of obtaining authorization) cloud service providers, and leverage existing authorizations to operate (ATOs) from other agencies to maximize savings; and
- Supporting GSA's objective to ensure that all systems which process, store, or transmit payment card data or purchase/credit card numbers are compliant with the current version of security requirements defined in the Payment Card Industry Data Security Standard (PCI DSS).

3. Federal Laws and Regulations. This Order provides policies that support the implementation of the following Federal laws, orders, directives, regulations, policies, standards, guidelines, commercial standards, and GSA directives:

- Federal Information Security Modernization Act (FISMA) of 2014 (Public Law 113-283)
- Clinger-Cohen Act of 1996 – Divisions D - Federal Acquisition Reform Act (FARA) and Division E – Information Technology Management Reform Act (ITMRA) of the National Defense Authorization Act of 1996 are collectively referred to as the Clinger-Cohen Act
- Chief Financial Officers (CFO) Act of 1990 (Public Law 101-576)
- 32 Code of Federal Regulations 2002, Controlled Unclassified Information
- Paperwork Reduction Act (PRA) of 1995 (Public Law 104-13)
- Federal Financial Management Improvement Act of 1996 (FFMIA) (Public Law 104-208)
- Federal Managers Financial Integrity Act of 1982 (FMFIA) (Public Law 97-255)
- Government Paperwork Elimination Act (GPEA) (Public Law 105-277)
- Privacy Act of 1974 (5 U.S.C. § 552a)
- Homeland Security Presidential Directive (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors

- Homeland Security Presidential Directive (HSPD-7), Critical Infrastructure Identification, Prioritization, and Protection
- Office of Management and Budget (OMB) Circular A-11, Preparation, Submission and Execution of the Budget
- OMB Circular A-130, Managing Information as a Strategic Resource
- OMB M-10-23, Guidance for Agency Use of Third-Party Websites and Applications
- OMB M-13-13, Open Data Policy -- Managing Information as an Asset
- OMB M-14-03, Enhancing the Security of Federal Information and Information Systems
- OMB M-16-16, 2016 Agency Open Government Plans
- OMB M-16-24, Role and Designation of Senior Agency Officials for Privacy
- OMB M-17-06, Policies for Federal Agency Public Websites and Digital Services
- OMB M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information
- OMB M-17-25, Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure
- OMB M-21-30, Protecting Critical Software Through Enhanced Security Measures
- OMB M-21-31, Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents
- OMB M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles
- Cybersecurity Enhancement Act of 2014
- PCI DSS (current version), Payment Card Industry Data Security Standard, Public Law No: 113-274.
- Presidential Policy Directive (PPD-21), Critical Infrastructure Security and Resilience
- EO 13556, Controlled Unclassified Information
- EO 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure
- EO 13873, Securing the Information and Communications Technology and Services Supply Chain
- EO 14028, Improving the Nation's Cybersecurity
- CSF, Version 1.1, Framework for Improving Critical Infrastructure Cybersecurity, April 16, 2018.
- Federal Information Processing Standard (FIPS) 140-3, Security Requirements for Cryptographic Modules, (Note: Although FIPS 140-3 has been issued, FIPS 140-2 modules are still being validated and will be accepted through September 22, 2026.)
- FIPS 199, Standards for Security Categorization of Federal Information and Information Systems
- FIPS 200, Minimum Security Requirements for Federal Information and Information Systems
- NIST Special Publications (SPs), GSA implements guidance provided by the NIST 800-series SPs within a year of guide publication, or as directed by the

CISO.
- NIST Security Measures for EO-Critical Software Use
- Office of Personnel Management (OPM) 5 Code of Federal Regulations (CFR) Part 930.301, Subpart C, Information Security Responsibilities for Employees who Manage or Use Federal Information Systems
- DHS CISA Cybersecurity Directives

4. GSA Policies:

- GSA Order ADM 2430.2, The U.S. General Services Administration Continuity of Operations Mission Essential Functions
- GSA Order ADM 7800.11A, Personal Use of Agency Office Equipment
- GSA Order ADM P 9732.1E, Personnel Security and Suitability Program Handbook
- GSA Order CIO 2200.1, GSA Privacy Act Program
- GSA Order CIO 1878.3 CHGE 1, Developing and Maintaining Privacy Threshold Assessments, Privacy Impact Assessments, Privacy Act Notices, and System of Records Notices
- GSA Order CIO P 2100.2C, GSA Wireless Local Area Network (LAN) Security
- GSA Order CIO 2101.2, GSA Enterprise Information Technology Management (ITM) Policy
- GSA Order CIO 2103.2, Controlled Unclassified Information (CUI) Policy
- GSA Order CIO 2104.1B CHGE 2, GSA Information Technology (IT) General Rules of Behavior
- GSA Order CIO 2110.4, GSA Enterprise Architecture Policy
- GSA Order CIO 2135.2D, GSA Policy for Information Technology (IT) Capital Planning and Investment Control (CPIC)
- GSA Order CIO 2140.4, Information Technology (IT) Solutions Life Cycle (SLC) Policy
- GSA Order OSC 2140.2A, Management of GSA's Digital Presence
- GSA Order CIO.2B CHGE 4, GSA Electronic Messaging and Related Services
- GSA Order CIO 2183.1, Enterprise Identity, Credential, and Access Management (ICAM) Policy
- GSA Order CIO 2231.1, GSA Data Release Policy
- GSA Order CIO 9297.2C CHGE 1, GSA Information Breach Notification Policy
- GSA Order CIO P 2165.2 CHGE 1, GSA Telecommunications Policy
- GSA Order CIO 2180.2, GSA Rules of Behavior for Handling Personally Identifiable Information (PII)
- GSA Order ADM 2181.1, Homeland Security Presidential Directive-12, Personal Identity Verification and Credentialing, and Background Investigations for Contractors
- GSA Order CIO 1821.2, GSA Records Management Program
- GSA Order OSC 2106.2, GSA Social Media Policy
- GSA CIO-IT Security Procedural Guides and Technical Guides and Standards
- GSAM Case 2021-G511, CHGE 135, GSA Acquisition Manual Case 2021-G511, Cyber-Supply Chain Risk Management (C-SCRM) Incident Response and Risk

Information Sharing, Change Order 135.

5. Compliance and Deviations.

a. Compliance is mandatory immediately upon the signing of this Order. This IT Security Policy requires all GSA SSOs including Regional Offices, Federal employees, contractors, and other authorized users of GSA's IT resources, to comply with the security requirements outlined in this policy. This policy must be properly implemented, enforced, and followed to effectively protect GSA's IT resources and data. Appropriate disciplinary actions must be taken in a timely manner in situations where individuals and/or systems are found non-compliant. Violations of this GSA IT Security Policy may result in disciplinary actions under GSA personnel policies and/or penalties under criminal and civil statutes.

b. All deviations from this Order must be approved by the appropriate Authorizing Official (AO) with a copy of the approval forwarded to the CISO in the Office of GSA IT for concurrence. Deviations must be documented using the Acceptance of Risk process defined in GSA CIO-IT Security-06-30, Managing Enterprise Risk, including a date of resolution to comply.

c. Additionally, any exceptions or deviations to GSA IT technical guides and standards shall follow the guidelines defined therein.

d. In the event of a disruption to normal operations (e.g., a lapse in appropriations) requirements in this directive will be extended until the disruption is resolved. For example, time based requirements (e.g., account disablement, ATO expiration) will have their time extended.

6. Maintenance. The GSA Office of the Chief Information Security Officer (OCISO) is required to review this policy at least annually and revise it to:

- Reflect any changes in Federal laws and regulations;
- Satisfy additional business requirements;
- Encompass new technology; and
- Adopt new Government IT standards.

7. Definitions. For the purposes of this Order the following terms are defined as listed.

a. Accountability. The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action.

b. Assurance. Substantiate with confidence that the other four security goals (integrity, availability, confidentiality, and accountability) have been adequately met by a specific implementation. “Adequately met” includes:

(1) Functionality that performs correctly,

(2) Sufficient protection against unintentional errors (by users or software), and

(3) Sufficient resistance to intentional penetration or by-pass.

c. Authorization. The official management decision given by a senior Federal official or officials to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security and privacy controls. Authorization also applies to common controls inherited by agency information systems.

d. Availability. Ensuring timely and reliable access to and use of information.

e. Confidentiality. Preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and CUI information. The property that sensitive information is not disclosed to unauthorized individuals, entities, or processes.

f. Critical Software. Critical software is defined as any software that has, or has direct software dependencies upon, one or more components with at least one of these attributes:

(1) is designed to run with elevated privilege or manage privileges;

(2) has direct or privileged access to networking or computing resources;

(3) is designed to control access to data or operational technology;

(4) performs a function critical to trust; or,

(5) operates outside of normal trust boundaries with privileged access.

g. Cybersecurity. Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

h. Federal Information System. An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.

(1) Contractor system. An information system in GSA's inventory processing or containing GSA or Federal data where the infrastructure and applications are wholly operated, administered, managed, and maintained by a contractor in non-GSA facilities.

(2) Federal system (i.e., Agency system). An information system in GSA's inventory system processing or containing GSA or Federal information where the infrastructure and/or applications are NOT wholly operated, administered, managed, and maintained by a Contractor.

i. Federal Information. Information created, collected, processed, maintained, disseminated, disclosed, or disposed of by or for the Federal Government, in any medium or form.

j. Integrity. Guarding against improper information modification or destruction and includes ensuring information nonrepudiation and authenticity. The property that sensitive data has not been modified or deleted in an unauthorized and undetected manner.

k. Major Information System. A system that is part of an investment requiring special management attention as defined in Office of Management and Budget (OMB) guidance and agency policies, a "major automated information system" as defined in 10 U.S.C. § 2445, or a system that is part of a major acquisition as defined in Part 7 of OMB Circular A-11, Capital Programming Guide, consisting of information resources.

l. Major IT Investment. An investment requiring special management attention as defined in OMB guidance and agency policies, a "major automated information system" as defined in 10 U.S.C. § 2445, or a major acquisition as defined in the OMB Circular A-11, Capital Programming Guide, consisting of information resources.

m. Minor Applications (Non-major Information Systems). Systems/applications that may be coalesced together as subsystems of a single larger, more comprehensive system for the purposes of security authorization. Minor applications/subsystems must be under the same management authority, have the same function or mission objective, the same operating characteristics, and information security needs, and reside in the same general operating environment(s).

n. Non-repudiation. Protection against an individual falsely denying having performed a certain action and provides the capability to determine whether an individual took a certain action such as creating information, sending a message, approving information, and receiving a message.

o. Personally Identifiable Information. Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

8. NIST SP (800 Series) and GSA Guidance Documents. All policies shall be implemented using the appropriate special publication from NIST and/or GSA procedural guides to the greatest extent possible. Where there is a conflict between NIST guidance and GSA guidance, contact the GSA OCISO for clarification. Where there are no procedural guides, use industry best practices (e.g., Center for Internet Security Benchmarks, Defense Information Systems Agency Benchmarks). Federal Information Processing Standards (FIPS) publication requirements are mandatory for use at GSA.

Deviations from compliance to NIST special publications must be documented and approved in the same manner as described in Chapter 1, Section 5 of this policy.

9. Privacy Act Systems. In addition to the security requirements in this Order, systems that contain Privacy Act data or PII must implement the privacy controls as defined in NIST SP 800-53 Revision 5 and GSA Order CIO 1878.3 CHGE 1.

10. IT Security Controls. All IT systems, including those operated by a contractor on behalf of the Government, must implement proper security controls according to:

a. Its security categorization level in IAW FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, and FIPS 200; and

b. NIST SP 800-53, Revision 5 (or subsequent revision based on GSA's implementation guidance for that revision).

11. Contractor Operations.

a. GSA System Program Managers and Contracting Officers shall ensure that the appropriate security requirements of this Order are included in task orders and contracts for all IT systems designed, developed, implemented, and operated by a contractor on behalf of GSA, including but not limited to systems operating in a Cloud Computing environment. In addition, GSA shall ensure that the contract allows GSA or its designated representative (i.e., third-party contractor) to review, monitor, test, and evaluate the proper implementation, operation, and maintenance of the security controls. This requirement includes, but is not limited to, documentation review, server configuration review, vulnerability scanning, code review, physical data center reviews, and operational process reviews and monitoring of Service Organization Control 2 and Statements on Standards for Attestation Engagements (SSAE) 18 reports.

b. The security controls implemented as part of contracts and task orders must include specific language requiring solutions to align with existing information security architecture. Security deliverables must be provided in a timely manner for review and acceptance by GSA. Additional information may be found in GSA CIO-IT Security-19-48, Security and Privacy Requirements for IT Acquisition Efforts and, for external information systems, in GSA CIO-IT Security-19-101, External Information System Monitoring. Note: As indicated in Chapter 1, Section 5, GSA has a deviation request

process by which a deviation from approved security architecture/standards may be requested.

12. Cybersecurity Framework.

a. EO 13800 requires all agencies to use the NIST CSF or any successor document to manage an agency's cybersecurity risk. To support this mandate, GSA has adapted this security policy and its primary procedural guides for managing risk, GSA CIO-IT Security-06-30, GSA CIO-IT Security-18-90, Information Security Program Plan, and Risk Management Strategy, and GSA CIO-IT Security-18-91 to align with the CSF. GSA is updating its security procedural guides (based on NIST SP 800-53, Revision 5 security control families) to show alignment with the CSF. This process will continue until all guides have been updated. The CSF is organized into five core CSF Functions:

- **Identify (ID):** Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.
- **Protect (PR):** Develop and implement appropriate safeguards to ensure delivery of critical services.
- **Detect (DE):** Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
- **Respond (RS):** Develop and implement appropriate activities to take action regarding a detected cybersecurity event.
- **Recover (RC):** Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

b. Chapters 3-7 of this policy are organized into the five core functions. Each chapter is further organized by the CSF's categories and subcategories which divide the functions into outcomes and activities. Appendix A details the category and subcategory definitions and unique identifiers. Additional information is available in CSF Version 1.1.

13. Cloud Services. No GSA user or SSOs including Regional Offices, shall conduct or acquire any type of pilot involving the use of GSA data or GSA logon credentials to a cloud service, platform, application, or tool without first consulting with the OCISO's Security Engineering Division (ISE). Such coordination can be made by contacting ISE representatives at SecEng@gsa.gov.

a. No procurement for such products/services shall be completed without coordination through the OCISO and having obtained a valid ATO granted by a GSA AO based on the processes defined in GSA CIO-IT Security-06-30 or a FedRAMP provisional ATO.

b. GSA users or SSOs may leverage GSA authorized Cloud Service Provider services reviewed by the GSA Security Engineering Division (ISE) and approved by the GSA CISO. Contact SecEng@gsa.gov for the current list of approved services.

c. The use of PII can only be involved in such products/services when the ATO grants such authorization specifically. PII shall never be introduced into any pilot program at any time.

d. Multi-Factor Authentication (MFA) shall be used when implementing any cloud service, application, or tool.

e. Privileged accounts must use MFA when accessing any cloud system via a network.

f. Non-privileged accounts must use MFA when accessing a FIPS 199 Moderate or High cloud system via a network.

g. Mobile applications that use a cloud platform for the storage, transmission, or processing of GSA data or Federal information under the management or control of GSA are subject to the above conditions.

14. Zero Trust. OMB M-22-09 establishes a Federal zero trust architecture (ZTA) strategy requiring agencies to meet specific cybersecurity standards and objectives. GSA has developed a Zero Trust Strategy Implementation Plan that aligns with the ZTA principles of NIST SP 800-207 and CISA's Zero Trust Maturity Model, including the five pillars listed below that support zero trust.

a. Identity - refers to a unique attribute or set of attributes describing an agency user or entity.

b. Devices - refers to any hardware asset that can connect to a network, including internet of things (IoT) devices, mobile phones, laptops, servers, and others.

c. Network - refers to an open communications medium, including agency internal networks, wireless networks, and the Internet, used to transport messages.

d. Workloads - include agency systems, computer programs, and services that execute on premise, as well as in a Cloud environment.

Data - refers to agency data on devices, in applications, and networks.

GSA's plan identifies two cross-capabilities that support the implementation of each of the pillar capabilities:

- **Automation and Orchestration**: Implements enforcement, testing, and repeatable configurations.
- **Data Analytics & Visualization**: Implements validation, trend analysis, and reporting for security monitoring.

Systems will be required to align with GSA's plan IAW the timelines and capabilities identified throughout it.

CHAPTER 2: SECURITY ROLES AND RESPONSIBILITIES

The roles and responsibilities described in the paragraphs below are assigned to the offices and positions identified to ensure effective implementation and management of GSA's IT Security Program. The establishment of a security management structure and assigning of security responsibilities is a requirement of the FISMA.

1. GSA Administrator. The Clinger-Cohen Act of 1996 assigns the responsibility for ensuring "that the information security policies, procedures, and practices of the executive agency are adequate" to the agency head. FISMA provides the following details on agency head responsibilities for information security:

a. Providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of an agency, and on information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

b. Ensuring that an information security program is developed, documented, and implemented to provide security for all systems, networks, and data that support the operations of the organization;

c. Ensuring that information security management processes are integrated with agency strategic and operational, and budgetary processes;

d. Ensuring that senior agency officials within the organization are given the necessary authority to secure the information and information systems that support the operations and assets under their control;

e. Designating a CIO and delegating authority to that individual to ensure compliance with applicable information security requirements;

f. Ensuring that the agency has trained personnel to support compliance with information security policies, processes, standards, and guidelines; and

g. Ensuring that the CIO, in coordination with the other senior agency officials, reports annually to the GSA Deputy Administrator on the effectiveness of the agency information security program, including the progress of remedial actions.

2. Risk Executive (Function). The Risk Executive (Function) at GSA is handled by the Enterprise Management Board (EMB), chaired by the Deputy Administrator who is also the Senior Accountable Official for Risk Management. For cybersecurity risks, the CISO, AOs, and subject matter experts facilitate the consistent application of risk management across GSA. The CISO coordinates with the CIO, a member of the EMB, to identify cybersecurity risks for consideration by the EMB. As stated in the EMB, the Risk

Executive (Function) manages and monitors key organizational risks, including those associated with enterprise-wide investments by:

a. Providing a forum to identify and discuss cross-cutting strategic, reputational, regulatory, operational, cybersecurity, financial, and other risks;

b. Elevating new or emerging risks and communicating the status of existing risks, including ongoing mitigation efforts;

c. Identifying risk owners and considering mitigation strategies and/or corrective actions;

d. Considering the effect of these efforts on new or ongoing resource allocation decisions;

e. Maintaining and maturing GSA's risk management framework, including its risk tolerance thresholds, risk appetite, and enterprise risk profile;

f. Engaging with other GSA governance groups, as needed, to provide strategic guidance;

g. Assigning action items to GSA Services and Staff Offices (SSOs) and their governance board for review and implementation;

h. Establishing risk management roles and responsibilities;

i. Developing and implementing an organization-wide risk management strategy that guides and informs organizational risk decisions (including how risk is framed, assessed, responded to, and monitored over time;

j. Determining organizational risk based on the aggregated risk from the operation and use of information systems and the respective environments of operation; and

k. Ensuring shared responsibility for supporting organizational missions and business functions using external providers receives the needed visibility and is elevated to appropriate decision-making authorities.

3. GSA CIO. Mandated by the Clinger-Cohen Act of 1996 and FISMA, the GSA CIO has overall responsibility for the GSA IT Security Program and reports to the GSA Deputy Administrator. Information security responsibilities include:

a. Developing and maintaining an agency-wide GSA IT Security Program;

b. Ensuring the agency effectively implements and maintains information security policies and guidelines;

c. Providing guidance, advice, and assistance to the Heads of Services and Staff Offices (HSSOs), and Regional Administrators on implementing GSA's IT Security Policy;

d. Providing management processes to enable AOs to implement the components of the IT Security Program for which they are responsible;

e. Ensuring information assurance and the protection of GSA's cyber-based critical infrastructure;

f. Ensuring senior agency officials, including CIOs of bureaus or equivalent officials, carry out their information security responsibilities for securing information and information systems supporting operations and assets under their control;

g. Ensuring all personnel are held accountable for complying with the agency-wide information security program, including taking actions when violations are identified IAW GSA Order HRM 9751.1, Maintaining Discipline.

h. Designating a CISO to assist in carrying out the GSA CIO's agency-wide IT security responsibilities;

i. Establishing reporting requirements within GSA to assess GSA's IT security posture, verifying compliance with Federal requirements and approved policies, and identifying agency-wide IT security needs;

j. Conducting independent activities and compliance reviews including oversight of GSA's Assessment and Authorization (A&A) process;

k. Coordinating and reporting on Presidential Policy Directive (PPD-21), Critical Infrastructure Security and Resilience critical infrastructure assets;

l. Reporting annually, in coordination with the other senior agency officials, to the GSA Deputy Administrator on the effectiveness of the agency information security program, including progress of remedial actions;

m. Ensuring Privacy Threshold Analyses (PTAs) and Privacy Impact Assessments (PIAs) prepared by GSA organizations for security considerations are reviewed;

n. Providing guidance or input for periodic assessments of SSOs including Regional Offices security measures and goals to assure implementation of GSA policy and procedures;

o. Participating as a member of the GSA Full Response Team IAW GSA Order CIO 9297.2C CHGE 1 to determine if a major incident has occurred;

p. Coordinating with the CISO and consulting with the Deputy Administrator, as necessary, regarding cybersecurity risks; and

q. Participating as a member of the EMB and coordinating with the CISO to identify cybersecurity risks for consideration by the EMB.

4. Chief Financial Officer (CFO). The CFO also has statutory security responsibilities under the Chief Financial Officers Act of 1990 and the Clinger-Cohen Act of 1996. Responsibilities include:

a. Developing and maintaining an integrated agency accounting and financial management system, including financial reporting and internal controls, which comply with the FMFIA and FFMIA requirements;

b. Complying with such policies and requirements as may be prescribed by the Director of OMB;

c. Complying with applicable accounting principles, standards, and requirements, and internal control standards and any other requirements applicable to such systems;

d. Supporting the GSA IT Capital Planning and Investment Control (CPIC) process. To achieve satisfactory assurance levels of information security for the financial systems of GSA, close cooperation between the offices of the CFO and the CIO is necessary, including supporting the GSA IT CPIC process; and

e. Reporting financial management information to OMB as part of the President's budget to include:

(1) Complying with legislative and OMB-defined responsibilities as they relate to IT capital investments; and

(2) Ensuring the appropriate security requirements of this Order are included in all contracts for IT systems designed, developed, implemented, and operated by a contractor that hosts GSA financial systems. This includes but is not limited to documentation review of operational processes and reviews that monitor SSAE 18 reporting submissions.

5. GSA Senior Agency Official for Privacy (SAOP). The SAOP has statutory responsibilities under the Privacy Act of 1974, GSA Order CIO 2200.1, OMB A-130, and OMB M-16-24. Information security responsibilities include:

a. Ensuring GSA information systems that contain PII address any recommendations of the SAOP as part of the system A&A, including addressing the privacy controls in NIST SP 800-53, Revision 5 as appropriate;

b. Ensuring that GSA data assets go through media protection processes IAW GSA CIO-IT Security-06-32, Media Protection (MP) prior to public release and that applicable Privacy Policies are followed;

c. Ensuring PTAs and PIAs are conducted for electronic information systems and collections and coordinating submission of all GSA Privacy Analysis Worksheets and PIA Summaries to OMB;

d. Developing, implementing, and overseeing personnel security controls for access to PII;

e. Directing the planning and implementation of the GSA Privacy Program to ensure agency personnel, including contractors, receive appropriate privacy awareness training based on their roles and access to privacy data; and

f. Participating as the GSA Full Response Team leader IAW GSA CIO Order 9297.2C CHGE 1 if a major incident involving privacy has occurred.

6. GSA Senior Agency Official (SAO) for CUI. The SAO for CUI is responsible for overseeing GSA's CUI Program. Information security responsibilities include:

a. Ensuring proper handling, marking, protection and destruction of all types of unclassified sensitive information;

b. Ensuring IT system and application owners conduct self-assessments to identify and mitigate potential risks to CUI; and

c. Determining if a CUI incident of misuse warrants an inquiry and reporting to the CUI Executive Agent.

7. GSA Chief Information Security Officer (CISO). FISMA establishes the designation of a Senior Agency Information Security Officer. GSA has assigned that responsibility to the CISO. The CISO is the focal point for all GSA IT security and must ensure the security requirements described in this Order are implemented agency-wide. The CISO reports directly to the CIO as required by FISMA. Responsibilities include:

a. Reporting to the GSA CIO on the implementation and maintenance of the GSA's IT Security Program and Security Policies;

b. Reporting to the GSA CIO on activities and trends that may affect the security of systems and applications assigned to GSA;

c. Implementing and overseeing GSA's IT Security Program by developing and publishing security policies and IT security procedural guides that are consistent with this policy;

d. Ensuring written agreements assign security-related functions and identify security responsibilities of each SSO including Regional Offices or activity when two or more activities use the same IT;

e. Providing guidance, advice, and assistance to all SSOs including Regional Officers, on IT security issues, the IT Security Program, and security policies;

f. Reporting to agency senior management on policy compliance;

g. Directing the planning and implementation of the GSA IT Security Awareness Training Program to ensure agency personnel, including contractors, receive appropriate security awareness training based on their roles and access to information and information systems;

h. Managing the OCISO which implements the GSA IT Security Program;

i. Establishing reporting deadlines for IT Security related issues requiring an agency response affecting the GSA IT Security Program;

j. Performing information security duties as the primary duty;

k. Assessing risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems supporting the operations and assets of the agency on a periodic basis;

l. Testing and evaluating the effectiveness of information security policies, procedures, and practices on a periodic basis;

m. Establishing and maintaining a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency;

n. Ensuring the development and implementation of procedures for detecting, reporting, and responding to security incidents;

o. Ensuring preparation and maintenance of plans and procedures to provide continuity of operations for information systems that support the GSA operations and assets;

p. Supporting the GSA CIO in annual reporting to the GSA Administrator on the effectiveness of the agency information security program, including progress of remedial actions;

q. Developing and implementing IT security performance measures to evaluate the effectiveness of technical and non-technical safeguards used to protect GSA information and information systems;

r. Assessing SSO including Regional Office, security measures and goals periodically to assure implementation of GSA policy and procedures;

s. Ensuring the appointment in writing of Information Systems Security Managers (ISSMs) and Information Systems Security Officers (ISSOs) for GSA systems;

t. Administering FISMA requirements and coordinating GSA's annual FISMA security program review and Plan of Action and Milestones (POA&M) implementations;

u. Ensuring IT Acquisitions align with GSA information security requirements;

v. Participating as the GSA Full Response Team leader, IAW GSA Order CIO 9297.2C CHGE 1 , if a major non-privacy incident has occurred;

w. Concurring/non-concurring on ATOs as specified in GSA CIO-IT Security-06-30 and its related A&A procedural guides;

x. Consulting with the Deputy Administrator, in coordination with the CIO, as necessary, regarding cybersecurity risks;

y. Coordinating with AOs and experts within the OCISO to apply consistent management of cybersecurity risks across GSA;

z. Providing authoritative decisions, or designating personnel to do so, in support of DevSecOps teams as specified in GSA CIO-IT Security-19-102, DevSecOps OCISO Program, and:

aa. Coordinating with the CIO to identify cybersecurity risks for consideration by the EMB.

8. HSSOs. Heads of Services and Staff Offices (HSSOs) are senior officials or executives within GSA with specific mission or line of business responsibilities. They are responsible for coordinating the efforts of management and technical personnel under their jurisdiction in meeting GSA IT Security requirements. Responsibilities include:

a. Ensuring that contractors performing services associated with GSA systems (such as system development, maintenance, or operation) are subject to GSA security requirements; and

b. Tracking the performance measures and goals established by the CISO and ensuring AOs, ISSMs, and ISSOs support these measures.

9. GSA Chief Privacy Officer (CPO). The CPO is responsible for overseeing GSA's Privacy Program. The CPO's mission is to preserve and enhance privacy protections for all individuals whose personal information is handled by GSA and to encourage

transparency of GSA operations involving personal information. The CPO reports to the SAOP. Information security responsibilities include:

a. Confirming that GSA information systems containing PII address any recommendations of the SAOP as part of the system A&A, including addressing the privacy controls in NIST SP 800-53, Revision 5, as appropriate;

b. Verifying that GSA data assets go through media protection processes IAW GSA CIO-IT Security-06-32 Media Protection (MP), prior to public release and that applicable privacy policies are followed;

c. Reviewing and approving PTAs and PIAs for electronic information systems and collections and coordinating submission of all GSA Privacy Analysis Worksheets and PIA Summaries to OMB;

d. Managing the implementation of personnel security controls for access to PII; and

e. Participating as a member of the GSA Full Response Team IAW GSA Order CIO 9297.2C CHGE 1.

10. Authorizing Official (AO). An AO is the Federal Government management official with the responsibility of identifying the level of acceptable risk for an information system, application, or set of common controls and determining whether an acceptable level of risk has been obtained. Final authority to operate or not operate for an information system, application, or a set of common controls rests with the AO. An AO must be assigned to every information system. An AO may have responsibility for more than one system, provided there is no conflict. Responsibilities include:

a. Reviewing and approving security safeguards of information systems and issuing ATO approvals for each information system, application, or set of common controls under their purview based on the acceptability of the implementation of security safeguards in place (risk-management approach);

b. Reviewing and approving all deviations and Acceptance of Risk (AoR) letters based on policies in this Order as described in Chapter 1, Section 5 of this Order;

c. Ensuring all information systems, applications, or sets of common controls under their purview have a current ATO issued IAW A&A processes defined in GSA CIO-IT Security-06-30 Managing Enterprise Cybersecurity Risk;

d. Ensuring ATO extensions are issued only based on the conditions identified in Chapter 3, Section 3.l and 3.m;

e. Ensuring vulnerability scans are able to be performed on information systems and applications under their purview IAW GSA CIO-IT Security-17-80: Vulnerability Management Process. Vulnerabilities identified from the scans shall be resolved and/or

tracked in the systems' POA&M IAW GSA CIO-IT Security-09-44: POA&M and GSA CIO-IT Security-06-30;

f. Providing support to the ISSMs and ISSOs appointed by the GSA CISO for GSA systems under their purview;

g. Ensuring cybersecurity is included in management planning, programming budgets, and the IT Capital Planning process;

h. Requiring point(s) of contacts (POCs) within other Federal agencies or outside organizations that manage GSA systems be maintained for systems under their purview. These POCs will be used for notification and coordination of security issues;

i. Ensuring IT systems handling privacy data meet the privacy and security requirements of the Privacy Act and IT information security laws and regulations. This includes GSA Order CIO 2200.1, GSA Order CIO 1878.3, and NIST SP 800-53, Revision 5;

j. Reviewing and approving PTAs/PIAs for information systems and applications under their purview;

k. Supporting the security measures and goals established by the CISO;

l. Ensuring all incidents involving data breaches which could result in identity theft are coordinated through OCISO and the GSA Full Response Team using the GSA breach notification plan per OMB M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information, GSA CIO-IT Security-01-02, Incident Response (IR), and GSA Order CIO 9297.2C CHGE 1;

m. Ensuring contingency plans are developed and tested annually IAW OMB Circular A-130, NIST SP 800-34, Revision 1, Contingency Planning Guide for Federal Information Systems, and GSA CIO-IT Security-06-29, Contingency Planning (CP);

n. Implementing detailed separation of duties policies for information systems and applications based on the specific processes, roles, permissions, and responsibilities of personnel involved in GSA business operations;

o. Establishing physical and logical access controls to enforce separation of duties policies and alignment with organizational and individual job responsibilities;

p. Ensuring access to information systems and applications by members of the GSA OIG as described in paragraph 19 of this chapter;

q. Establishing, where appropriate, system/organization unique rules of behavior for information systems and applications under their purview;

r. Ensuring information systems and applications handling payment card data meet the security requirements of the PCI DSS; and

s. Coordinating with the CISO and experts within the OCISO regarding the consistent management of cybersecurity risks across GSA.

11. Office of CISO Division Directors. OCISO Directors serve as an intermediary to the AO for ensuring security is implemented. The Directors are the focal point for all IT system security matters for the IT resources under their responsibility. OCISO Directors report to the CISO. Responsibilities include:

a. Monitoring adherence and proper implementation of GSA's IT Security Policy and reporting the results to the CISO;

b. Reviewing and approving A&A documents to be signed by the appropriate business line representatives and concurred by the CISO or appropriate OCISO personnel;

c. Ensuring the security measures and goals established by the CISO are met by the organizations under their responsibility;

d. Ensuring GSA security awareness training requirements for individuals under their responsibility are complied with;

e. Creating security policies that achieve compliance to appropriately address new security requirements;

f. Advising individuals with IT Security responsibilities on proper system security, security "Best Practices," and applicable laws and regulations;

g. Assisting individuals with IT Security responsibilities on security architecture and security engineering principles and practices;

h. Interfacing with the Technical Standards Committee regarding security;

i. Developing, implementing, and tracking the collection of data and reporting of status on POA&Ms, FISMA requirements, and other external or internal requests or requirements (e.g., Government Accountability Office (GAO), OIG);

j. Coordinating the designation, documentation, and inheritance of common controls with individuals who have IT Security responsibility for information systems;

k. Coordinating the implementation of on-going authorization and continuous monitoring processes with individuals with IT Security responsibility for information systems;

l. Coordinating with System Owners, ISSMs, and ISSOs to maintain an accurate inventory of GSA information systems (including hardware, software, and other data required by Federal or GSA requirements) in the GSA official system inventory repository;

m. Developing and implementing procedures for detecting, reporting, and responding to security incidents;

n. Managing an OCISO Division to implement the GSA IT Security Program;

o. Appointing ISSMs and ISSOs in writing for GSA systems;

p. Participating as a member of the GSA Full Response Team (ISE Division Director) as defined in GSA Order 9297.2C CHGE 1 to determine if a major incident has occurred. The ISE Division Director may designate a representative to fulfill this responsibility on a case-by-case basis; and

q. Collaborating with system personnel and others, as required, to collect data and report to OMB, DHS, or other Federal authorities information regarding cybersecurity (e.g., CISA directives, the Cybersecurity Coordination, Assessment, and Response Protocol [C-CAR], critical software).

12. ISSM. The ISSM serves as an intermediary to the system owner and the OCISO Director responsible for ISSO services. There is at least one ISSM per AO. The ISSM reports to the OCISO IST Director for the systems under their purview. An individual appointed as ISSM for a system cannot also be assigned as the ISSO for the same system. ISSMs must be Federal employees. The ISSO Support Division (IST) facilitates integrating IT security in programs and compliance with required security and privacy requirements. The GSA official system inventory repository contains a current list of ISSMs. Responsibilities include:

a. Providing guidance, advice, and assistance to ISSOs on IT security issues, the IT Security Program, and security policies;

b. Verifying annually the list of ISSOs and providing an updated designation letter to the Director for submission to the CISO when changes occur or designations expire;

c. Ensuring A&A support documentation is developed and maintained for the life of the system, including the usage of GSA's implementation of the Archer Governance, Risk, and Compliance (GRC) solution;

d. Reviewing ISSO checklists submitted in Archer GRC and coordinating with ISSOs, as necessary, for systems under their purview;

e. Reviewing and coordinating reporting of Security Advisory Alerts (SAAs), compliance reviews, security awareness training, incident reports, contingency plan testing, and other IT security program elements;

f. Managing system assessments (including A&A package requirements and PCI DSS Report on Compliance [for IT systems that process, store, or transmit payment card data or purchase/credit card numbers]), and forwarding them to the AO and appropriate OCISO Directors;

g. Forwarding to the applicable OCISO Director, copies of A&A documents to be signed by the appropriate individuals as required in A&A guidance;

h. Supporting the security measures and goals established by the CISO;

i. Complying with GSA security awareness training requirements for individuals with significant security responsibilities; and

j. Working with the ISSO and system owner to develop, implement, and manage POA&Ms for their respective systems IAW GSA CIO-IT Security-09-44.

13. ISSO. The ISSO is responsible for ensuring implementation of adequate system security to prevent, detect, and recover from security breaches. An ISSO must be assigned for every information system. An ISSO may have responsibility for more than one system, provided there is no conflict. An individual assigned as the ISSO cannot also be the ISSM or system owner for the same system. ISSOs may be Federal employees or contractors. The ISSO must be knowledgeable of the information and processes supported by the system. ISSO Checklists consisting of recurring tasks ISSOs must perform are managed in GSA's implementation of Archer GRC; ISSOs receive notification to complete checklists when they are generated. A current list of ISSOs is located in the GSA official system inventory repository, GSA EA Analytics and Reporting. Responsibilities include:

a. Ensuring the system is operated, used, maintained, and disposed of IAW documented security policies and procedures. Necessary security controls should be in place and operating as intended;

b. Advising System Owners of risks to their systems and obtaining assistance from the ISSM, if necessary, in assessing risk;

c. Assisting system owners in completing and maintaining the appropriate A&A documentation as specified in GSA CIO-IT Security-06-30, including the usage of Archer GRC;

d. Completing the recurring activities in ISSO checklists, completing the checklists in Archer GRC, and submitting the checklists when completed;

e. Assisting the AO, data owner and Contracting Officer (CO)/Contracting Officer Representative (COR) in ensuring users have the required background investigations, the required authorization and need-to-know, and are familiar with internal security practices before access is granted to the system;

f. Promoting information security awareness;

g. Identifying, reporting, and responding to information security incidents in coordination with GSA's incident responders, including beginning protective and corrective measures as directed;

h. Ensuring the user identification and authentication scheme used in the system is administered as intended, including reviewing system role assignments to validate compliance with principles of least privilege;

i. Ensuring media protection procedures are followed IAW GSA CIO-IT Security-06-32;

j. Reviewing audit/log reports for systems integrated with the GSA Enterprise Logging Platform (ELP) for potential security issues;

k. Verifying systems not integrated with the GSA ELP/audit logging tool perform similar reviews to identify potential security issues;

l. Evaluating SAAs and known vulnerabilities to ascertain if additional safeguards are needed and ensuring systems are patched and securely configured, as appropriate;

m. Supporting the security measures and goals established by the CISO;

n. Complying with GSA security awareness training requirements for individuals with significant security responsibilities;

o. Assisting the AO in achieving PCI DSS implementation and compliance for IT systems that process, store, or transmit payment card data, to include creating and maintaining PCI DSS documentation, and facilitating the self-assessment;

p. Assisting in the identification, implementation, and assessment of a system's security controls, including common controls;

q. Coordinating with the OCISO to maintain an accurate inventory of GSA information systems (including hardware, software, and other data required by Federal or GSA requirements) in the GSA official system inventory; and

r. Working with the system owner and ISSM to develop, implement, and manage POA&Ms for their respective systems IAW GSA CIO-IT Security-09-44.

14. System Owners. System Owners are management officials within GSA with responsibility for the acquisition, development, maintenance, implementation, and operation of GSA's IT systems. System Owners cannot be ISSOs or ISSMs. System Owners represent the interests of the system throughout its lifecycle. Primary responsibility for managing risk should rest with the System Owners. Responsibilities include:

a. Ensuring systems and the data each system processes have necessary security controls in place and are operating as intended and protected IAW GSA regulations and any additional guidelines established by the OCISO and relayed by the ISSO or ISSM;

b. Obtaining the resources necessary to securely implement and manage their respective systems;

c. Consulting with the ISSM and ISSO and receiving the approval of the AO, when selecting the mix of controls, technologies, and procedures that best fit the risk profile of the system;

d. Participating in activities related to the A&A of the system to include security planning, risk assessments, security and incident response testing, configuration management, and contingency planning and testing;

e. Coordinating with the OCISO and the ISSO to maintain an accurate inventory of GSA information systems (including hardware, software, and other data required by Federal or GSA requirements) in the GSA official system inventory;

f. Defining and scheduling software patches, upgrades, and system modifications;

g. Ensuring IT security and privacy requirements are included in IT contracts or contracts including IT;

h. Conducting PTAs on all systems to ascertain whether the system collects information on individuals or when new systems are developed, acquired, or purchased; performing PIAs when applicable;

i. Developing, implementing, and maintaining an approved IT contingency plan which includes an acceptable Business Impact Analysis (BIA);

j. Ensuring that information and system categorization has been established for their systems and data IAW FIPS 199, Standards for Security Categorization of Federal Information and Information Systems;

k. Conducting annual reviews and validation of system users' accounts to ensure the continued need for access to a system and verify users' authorizations (rights/privileges);

l. Ensuring security is planned, documented, and integrated into the system development life cycle from the information system's initiation phase to the system's disposal phase;

m. Reviewing the security controls for their systems and networks annually as part of the FISMA self-assessment, when significant changes are made to the system and network, and at least every three years or via continuous monitoring if the system is in GSA's information security continuous monitoring program;

n. Defining, implementing, and enforcing detailed separation of duties by ensuring single individuals do not have control of the entirety of a critical process, roles, permissions, and/or responsibilities;

o. Ensuring physical or environmental security requirements are implemented for facilities and equipment used for processing, transmitting, or storing sensitive information based on the level of risk;

p. Obtaining a written ATO following GSA A&A processes prior to making production systems operational and/or Internet accessible. Developing and maintaining the system security plan and ensuring that the system is deployed and operated according to the agreed-upon security requirements;

q. Ensuring system users and support personnel receive the requisite security awareness training (e.g., instruction in system rules of behavior);

r. Supporting the security measures and goals established by the CISO;

s. Complying with GSA security awareness training requirements for individuals with significant security responsibilities;

t. Integrating and explicitly identifying security funding for information systems and programs into IT investment and budgeting plans;

u. Coordinating with IT security personnel, including the ISSM and ISSO and Data Owners, to ensure implementation of system and data security requirements;

v. Working with the ISSO and ISSM to develop, implement, and manage POA&Ms for their respective systems IAW GSA CIO-IT Security-09-44;

w. Ensuring proper separation of duties for GSA IT system maintenance, management, and development processes;

x. Conducting annual assessments to review the effectiveness of control techniques, with an emphasis on activities that cannot be controlled through logical, physical, or compensating controls;

y. Working with the Data Owner, granting access to the information system based on a valid need-to-know/need-to-share that is determined during the account authorization process and the intended system usage;

z. Working with Data Owners to ensure the appropriate level of auditing and logging data is enabled and generated to support monitoring activities, and supports GSA's plan to comply with OMB M-21-31 active and cold data storage time frames;

aa. Working with Data Owners to audit user activity for indications of fraud, misconduct, or other irregularities;

bb. Working with Data Owners to document all phases of monitoring activity including monitoring procedures, response processes, and steps performed when reviewing user activity;

cc. Reviewing the security requirements for systems and networks which are in-scope of PCI DSS annually as part of the PCI DSS assessment and when significant changes are made to the system and network;

dd. Working with the OCISO and Data Owners to respond to any information security incidents that impact the system or the data stored within the system;

ee. Participating as a member of the GSA Full Response Team as defined in GSA Order 9297.2C CHGE 1 to determine if a major incident has occurred; and

ff. Managing DevSecOps teams implemented for their systems in collaboration with OCIOS assigned DevSecOps engineer.

15. Program Managers. Program Managers are management officials within GSA who are responsible for developing, implementing, and/or overseeing multi-year IT initiatives that must be carried out through multiple related projects. A program manager focuses on the strategic goals of GSA. Their role is to manage several related projects in a coordinated manner to attain strategic results that could not be achieved at the individual project level. Responsibilities include:

a. Ensuring the appropriate security requirements of this Order are included in task orders and contracts for all IT systems designed, developed, implemented, and operated by a contractor on behalf of the Government;

b. Ensuring cyber risk is adequately managed within the projects under their purview IAW GSA CIO-IT Security-18-90, GSA CIO-IT Security-18-91, and GSA CIO-IT Security-06-30;

c. Coordinating the projects under their purview to ensure resources are allocated, monitored, and managed to support the required level of security; and

d. Participating as a member of the GSA Full Response Team as defined in GSA Order CIO 9297.2C CHGE 1 to determine if a major incident has occurred for a system under their purview.

16. Project Managers. Project Managers are management officials within GSA who are responsible for managing a project within a larger program. A Project Manager focuses on managing a team to achieve the goals of the project. Responsibilities include:

a. Ensuring GSA IT security policies and procedural requirements are integrated and cyber risk is adequately managed within projects under their purview IAW GSA CIO-IT Security-18-91 and GSA CIO-IT Security-06-30; and

b. Managing the schedule, resources, and tasks within a project, ensuring security is delivered.

17. Data Owners. The Data Owner/Functional Business Line Manager owns the information but not the system, application, or platform on which the information is stored, transmitted, or processed. Responsibilities include:

a. Determining the security categorization of systems based upon the FIPS 199 levels and ensuring that System Owners are aware of the sensitivity of data to be handled;

b. Coordinating with System Owners, ISSMs, ISSOs, and Custodians to ensure the data is properly stored, maintained, and protected IAW GSA policies, regulations and any additional guidelines established by GSA;

c. Working with the System Owner, with assistance from the ISSO, to ensure system access is restricted to authorized users that have completed required background investigations, are familiar with internal security practices, and have completed requisite security awareness training programs (e.g., the annual IT Security and Privacy Awareness course);

d. Reviewing access authorization listings and determining whether they remain appropriate at least annually;

e. Ensuring protection of GSA's systems and data IAW GSA's IT Security Policy and the GSA Records Management Program;

f. Ensuring that data is not processed on a system with security controls that are not commensurate with the sensitivity of the data;

g. Assisting in identifying and assessing common security controls where the information resides;

h. Ensuring information systems that allow authentication of users for the purpose of conducting Government business electronically complete a Digital Identity Acceptance Statement for digital transactions resulting in an assurance level classification IAW NIST SP 800-63-3, Digital Identity Guidelines;

i. Coordinating with IT security personnel including the ISSM and ISSO and system owners to ensure implementation of system and data security requirements;

j. Working with the system owner to ensure the appropriate level of auditing and logging data is enabled and generated to support monitoring activities, and supports GSA's plan to comply with OMB M-21-31 active and cold data storage time frames;

k. Working with the system owner to audit user activity for indications of fraud, misconduct, or other irregularities;

l. Working with the system owner to document all phases of monitoring activity including monitoring procedures, response processes, and steps performed when reviewing user activity;

m. Identifying the data assets to catalog in GSA's Enterprise Data Inventory (EDI) and for possible public release; and

n. Working with the OCISO and system owner to respond to any information security incidents that impact a system or the data stored within a system.

18. Contracting Officer (CO) and CO Representative (COR). The CO/COR function is responsible for managing contracts and overseeing their implementation. Personnel executing this function have the following information security responsibilities:

a. Collaborating with the CISO or other appropriate official to ensure the agency's contracting policies adequately address the agency's information security requirements;

b. Coordinating with the CISO or other appropriate official as required, to ensure that all agency contracts and procurements comply with the agency's information security policy, and include appropriate security contracting language and security requirements in each contract;

c. Ensuring that all personnel with responsibilities in the agency's procurement process are properly trained in information security;

d. Working with the CISO to facilitate the monitoring of contract performance for compliance with the agency's information security policy;

e. Identifying, initiating, and adhering to favorable enter on duty requirements for contractor background investigations in collaboration with the GSA Personnel Security Officer/Office of Mission Assurance (OMA);

f. Ensuring contracts and task orders for ISSM and ISSO services include measurable performance requirements;

g. Maintaining the integrity and quality of the proposal evaluation, negotiation, and source selection processes while ensuring that all terms and conditions of the contract are met;

h. Ensuring industry and Government IT providers use Security Content Automation Protocol validated tools with the United States Government Configuration Baseline (USGCB) scanner capability to certify their products operate correctly with USGCB configurations and do not alter USGCB settings; and

i. Ensuring new solicitations for all GSA IT systems include the security contract language from GSA CIO-IT Security-09-48.

19. Custodians. Custodians own the hardware platforms and equipment on which the data is processed. They are the individuals in physical or logical possession of information from Data Owners. Responsibilities include:

a. Coordinating with data owners and system owners to ensure the data is properly stored, maintained, and protected;

b. Providing and administering general controls such as back-up and recovery systems consistent with the policies and standards issued by the Data Owner;

c. Establishing, monitoring, and operating information systems in a manner consistent with GSA policies and standards as relayed by the AO;

d. Accessing data only on a need-to-know basis as determined by the Data Owner; and

e. Providing the OCISO with physical access to devices when needed as part of any incident response effort.

20. Authorized Users of IT Resources. Authorized users of GSA IT resources, including all Federal employees and contractors, either by direct or indirect connections, are responsible for complying with GSA's IT Security Policy and procedures. Their responsibilities include:

a. Complying with security awareness training and education sessions commensurate with their duties;

b. Reporting any observed or suspected security problems/incidents to the IT Service Desk;

c. Familiarizing themselves with any special requirements for accessing, protecting, and using CUI data, including Privacy Act requirements, copyright requirements, and procurement-sensitive data;

d. Ensuring adequate protection is maintained on their workstation, including not sharing passwords with any other person and logging out, locking, or enabling a password protected screen saver, and removing their PIV card before leaving their workstation;

e. Accessing systems and data only on a need-to-know, need-to-use, and need-to-share basis;

f. Utilizing assigned privileged access rights (e.g., administrator, power user, database administrator, web site administrator, etc.) to a computer based on need-to-use (i.e., using accounts with those privileges only when the privileges are required to complete an action);

g. Ensuring any sensitive data (e.g., PII, PCI, CUI, authenticators, business sensitive data) stored on any workstations or mobile devices including, but not limited to, laptop computers, notebook computers, external hard drives, USB drives, CD-ROMs/DVDs, and personal digital assistants, are encrypted with GSA-provided encryption;

h. Ensuring PII/CUI data is only accessed remotely from GFE or through an approved GSA virtual interface (i.e., Citrix and/or VDI). Note: Remote access is permitted unless a system's AO or SAOP explicitly prohibit such access; and

i. Ensuring PII/CUI data is not downloaded or stored on non-GFE.

21. GSA Office of Inspector General (IG). The GSA OIG is a statutory office within GSA that, in addition to other responsibilities, works to assess an organization's information security practices and identifies vulnerabilities and the possible need to modify security measures. The OIG completes this task by:

a. Detecting fraud or instances of waste, abuse, or misuse of an organization's funds;

b. Identifying operational deficiencies within the organization;

c. Performing annual independent FISMA evaluations IAW 44 U.S.C. § 3555(b)(1);

d. Accessing GSA and contractor records. OIG auditors, investigators, inspectors, and attorneys must be provided access to all records, reports, reviews, documents, papers, and materials available to GSA and pertaining to agency programs and activities. When performing reviews of contractor records and proposals, access to information is provided by statute, contract terms, and agreements between the

contractor and the Government. To facilitate the process of gaining access to information, auditors, investigators, inspectors, and attorneys carry credentials identifying them as OIG officials. In addition, the following procedures will be followed to allow OIG personnel access to GSA information systems:

(1) For the OIG, the point of contact will be the Assistant Inspector General for Auditing (AIGA) or the AIGA's designees. For the SSOs within GSA, the points of contact will be the AO for each information system;

(2) The AIGA will notify the AO of the information system within the AIGA's purview which OIG personnel need to access;

(3) The AO will inform the AIGA of the highest classification level of information on the system and all required security and privacy awareness training required for GSA and/or contractor personnel to access the system;

(4) The AIGA will designate the OIG personnel who are to be given access and ensure they have appropriate clearance levels;

(5) The AIGA will certify that each OIG person who may have access to the system has completed all security and privacy awareness training required of GSA personnel before access is granted;

(6) The AIGA will annually certify that each OIG person with access to a GSA system has a continuing need for access and has maintained up-to-date training requirements in connection with the system owner's annual review and validation of systems users' accounts;

(7) The AIGA will ensure and state that access is necessary for OIG personnel to accomplish assigned tasks IAW the OIG's organizational mission and functions. The following statement from the AIGA will suffice to establish that access is necessary for these purposes: "This access is requested to fulfill the OIG's statutory responsibility to conduct and supervise audits, inspections, and investigations relating to the programs and operations of GSA, and to promote economy, efficiency, and effectiveness in the administration of, and to prevent and detect fraud, waste, and abuse in GSA programs and operations;"

(8) Regarding requests for access to Privacy Act systems of records, the AIGA will ensure and certify that the OIG personnel who will be accessing the system have a need for the records in the performance of their duties. The statement shall suffice to establish that access to the system is consistent with the requirements of the Privacy Act;

(9) The AO will work with the system owner to ensure access is granted promptly after the above steps have been completed. If access cannot be granted within 14 calendar days after completion of the above steps, the AO will inform the HSSO and

the AIGA and will work with the AIGA to resolve any impediments to OIG access to the system. The CIO, or designee, will assist as requested in resolving any issues;

(10) The system owner will authorize OIG personnel to access GSA-owned information systems from the OIG's accredited system. When possible under contractual terms, OIG personnel will be authorized access to contractor-owned information systems from the OIG's accredited system;

(11) To the extent practicable, OIG personnel will not be granted access to other agencies' owned or controlled records or information about other agencies and their employees that may be maintained in a GSA-controlled system, absent the other agency's permission;

(12) The OIG will advise the AO immediately if circumstances change such that access is no longer needed; for example, if an individual with access leaves the OIG, or upon conclusion of the investigation/inspection/audit or other OIG purpose for which systems access was provided;

(13) OIG employees will have "read-only" access to all information in the system. OIG personnel will not be able to add to, delete, or modify the data in the system;

(14) Each OIG employee with access will use a unique identifier and password when accessing the system;

(15) Testing in support of an OIG review, whether manual or automated, shall not have an adverse effect on the operational production status of the IT system being reviewed other than the increase in usage/traffic due to additional users;

(16) OIG operational needs may preclude OIG staff from obtaining the required approvals prior to removal of PII from GSA facilities. The following statement from the AIGA will suffice to establish that requirement is necessary for these purposes: "This access is requested to fulfill the OIG's statutory responsibility to conduct and supervise audits, inspections, and investigations relating to the programs and operations of GSA, and to promote economy, efficiency and effectiveness in the administration of, and to prevent and detect fraud, waste, and abuse in, GSA programs and operations;" and

(17) Should the system be compromised by a reportable incident, and the access of OIG personnel be implicated in the incident, the system owner will promptly notify the IG in writing, and the IG will take appropriate action with respect to the employee(s) responsible.

22. GSA Personnel Security Officer, OMA. The GSA personnel security officer is responsible for the overall implementation and management of personnel security controls across GSA, to include integration with specific information security controls. In

consideration of information security, the personnel security officer has responsibility for:

a. Developing, promulgating, implementing, and monitoring GSA personnel security programs;

b. Developing and implementing access agreements, and personnel screening, termination, and transfer procedures; and

c. Ensuring consistent and appropriate sanctions for personnel violating management, operation, or technical information security controls.

23. Office of Human Resources Management (OHRM). The Human Resource Office and Security Office are responsible for designating the risk levels for all occupations in GSA and incorporate the risk level in the position designation(s) for each series and grade.

24. System/Network Administrators. System/network administrators are responsible for:

a. Ensuring the appropriate security requirements are implemented consistent with GSA IT security policies and hardening guidelines;

b. Implementing system backups and remediation of security vulnerabilities, including patching, updates, configuration changes, etc.;

c. Utilizing privileged access rights (e.g., “administrator,” “root,” etc.) to a computer based on a need-to-use basis (i.e., using accounts with those privileges only when the privileges are required to complete an action);

d. Working with the custodian/ISSO to ensure appropriate technical security requirements are implemented;

e. Ensuring system/network administrators have separate administrator and user accounts, if applicable (e.g., Microsoft Windows accounts). A normal user account should be used unless administrator rights are required to perform a job function;

f. Identifying and reporting security incidents and assisting the OCISO in resolving the security incident;

g. Utilizing GSA provided MFA to ensure strong authentication; and

h. Performing audit/log reviews for systems not integrated with the GSA ELP to identify potential security issues as specified in the system’s system security plan (SSP).

25. Supervisors. Supervisors are responsible for:

a. Conducting annual review and validation of staff user accounts to ensure the continued need for access to a system;

b. Conducting annual reviews of staff training records to ensure annual IT Security and Privacy Awareness Training, and application specific training has been completed for all users. The records shall be forwarded to ISSOs/system owners as part of the annual recertification efforts;

c. Coordinating and arranging system access requests for all new or transferring employees and verifying an individual's need-to-know (authorization);

d. Coordinating and arranging system access termination for all terminating or transferring personnel;

e. Coordinating and arranging system access modifications for personnel; and

f. Documenting job descriptions and roles to accurately reflect the assigned duties, responsibilities, and separation of duties principles. Establishing formal procedures to guide personnel in performing their duties, with identification of prohibited actions.

26. OCISO DevSecOps Program (ODP) Security Engineer. ODP Security Engineers are responsible for:

a. Collaborating with the system team on all aspects of system security;

b. Engaging on solution design, planning, and criteria for security requirements;

c. Interpreting security requirements from policies and standards and their applicability to the development project;

d. Integrating security analysis into the change management processes;

e. Collaborating on security code review and compliance impact analysis; and

f. Acting as liaison with the OCISO for decisions and approvals.

CHAPTER 3: POLICY FOR IDENTIFY FUNCTION

This chapter provides security policy statements for the CSF Identify function, which allows GSA to develop an understanding of its systems, assets, data, and capabilities to manage cybersecurity risk. Use of the activities in the Identify function will enable GSA to prioritize its efforts consistent with its risk management strategy and business needs, by understanding the business context, the resources supporting critical functions, and related cybersecurity risks.

The following paragraphs provide the specific policy statements supporting outcomes for the CSF Identify categories and subcategories. Appendix A details specific Identify Category and Subcategory definitions and unique identifiers.

1. Asset Management.

a. Inventories of physical devices/components of information systems will be maintained IAW GSA CIO-IT Security-01-05, Configuration Management (CM).

b. An accurate inventory of GSA information systems (including hardware, software, and other data required by Federal or GSA requirements) will be maintained in GSA's official system inventory repository.

c. IAW OMB M-21-30 and NIST's Security Measures for EO-Critical Software Use webpage:

(1) GSA must maintain a critical software inventory.

(2) Critical software must implement the security measures defined on NIST's webpage.

d. All interconnections between GSA and external entities including off-site contractors or Federal agency/departments must be documented in an Interconnection Security Agreement (ISA) that is approved by the AOs and concurred by the GSA CISO. ISAs must, at a minimum, be reviewed annually. See NIST SP 800-47, Revision 1, Managing the Security of Information Exchanges, for detailed information.

e. All communications and data flows, internal and external, for an information system must be documented in the System Security Plan (SSP).

f. All system interconnections, including connections to external systems, must be documented in the SSP.

g. All information systems must comply with NIST SP 800-60, Volume 1, Revision 1, Guide for Mapping Types of Information and Information Systems to Security Categories, and FIPS 199, Standards for Security Categorization of Federal Information

and Information Systems, to determine their security category (i.e., potential impacts for confidentiality, availability, and integrity).

h. As part of a system's contingency planning process, resources must be prioritized based on their classification, criticality, and business value. A BIA is required as part of the system's contingency plan.

i. All GFE, including PIV cards, must be returned to GSA at the end of a contract and when contract personnel no longer support a contract and as directed by a Contracting Officer.

j. Per OMB M-17-06, only an approved .gov or .mil domain may be used for official public-facing websites.

2. Business Environment.

a. GSA's roles within the supply chain are: (1) as a consumer of supplies from vendors/providers for its internal systems and use; and (2) as an acquisition agency dedicated to procuring goods and services for the Federal Government, as well as providing acquisition, technical, and project management services to assist agencies in acquiring and deploying information technology and professional services solutions.

b. In both roles identified in the previous paragraph, requiring activities, working with their COs must ensure supply chain risk management is included in contracts where appropriate, and acquirers must determine whether the acquisition risk is acceptable given their system's environment.

c. Per PPD-21 GSA, in consultation with the Department of Defense (DOD), DHS, and other departments and agencies as appropriate, shall provide or support government-wide contracts for critical infrastructure systems and ensure that such contracts include audit rights for the security and resilience of critical infrastructure.

d. GSA system contingency plan's BIA should prioritize business missions in relation to the systems supporting the mission objectives and activities.

e. GSA system contingency plan's BIA should identify critical services and any dependencies regarding those services.

f. Integrate and explicitly identify funding for information systems and programs into IT investment and budgeting plans per GSA Order CIO 2135.2D, GSA Policy for IT Capital Planning and Investment Control. GSA's capital planning and investment control process must be used for the continuous selection, control, and evaluation of IT investments over their lifecycles.

g. GSA HSSOs must ensure key personnel have the capacity to perform Mission Essential Functions (MEFs) and Essential Supporting Activities to maintain agency

resiliency and directly support the public IAW GSA Order ADM 2430.2, The U.S. General Services Administration Continuity of Operations Mission Essential Functions.

h. GSA system contingency plans must address the ability to continue missions under all operating states (e.g., disasters/attacks, recovery, and restoration to normal operations).

3. Governance.

a. This policy, GSA Order CIO 2100.1, outlines GSA's information security policy.

b. HSSOs, system owners, and others as specified in Chapter 2, must ensure personnel are assigned to fulfill the roles and perform the responsibilities for systems under their purview, including contractor/vendor systems.

c. The primary focus of GSA Order CIO 2100.1 is to provide guidelines that support the implementation of Federal regulations and laws, and the latest versions of the GSA directives referenced in this policy. Chapter 1, Section 3, Federal Laws and Regulations, lists references to legal and regulatory guidance supported by this policy.

d. An entity-wide IT security program must include compliance reviews to determine how well the overall GSA security program meets the agency performance measures.

e. All GSA information systems must complete a PTA and a PIA as part of the A&A process. The PTA/PIA must be reviewed and updated annually or more frequently if there is a significant change to the system's privacy posture. PTAs/PIAs must be prepared IAW GSA Order CIO 1878.3 CHGE 1.

f. The OCISO must submit, on behalf of the CIO, an agency-wide FISMA Report to OMB and specified congressional committees annually.

g. The OCISO will generate and store records created or received in the course of performing information security management IAW GSA Order OAS P 1820.1, GSA Records Management Program.

h. AOs must implement a risk management process for all information systems using NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View, NIST SP 800-30 Revision 1, Guide for Conducting Risk Assessments, GSA CIO-IT Security-06-30, and A&A process procedural guides as required.

i. AOs must ensure risk assessments are performed and documented as part of A&A activities IAW GSA CIO-IT Security-06-30:

(1) Before a system is placed into production;

(2) When significant changes are made to the system;

(3) At least every three (3) years; or

(4) Via continuous monitoring based on continuous monitoring plans reviewed and accepted by the GSA CISO.

j. The OCISO must conduct compliance reviews to determine if risk is being properly addressed IAW with GSA CIO-IT Security-06-30, GSA CIO-IT Security-18-91, and GSA CIO-IT Security-18-90.

k. All information systems must be authorized, in writing, before they go into operation. The authorization must be IAW one of the A&A processes in GSA CIO-IT Security-06-30 which requires the system and its risks to be assessed and reported in A&A/ATO packages. The A&A/ATO packages, and therefore system risks, must be updated IAW the system's specific A&A process schedule.

l. Authorizations can be granted with or without restrictions or limitations. Authorizations with restrictions must identify in the ATO package's Certification and ATO Letters the conditions needing to be resolved and their associated POA&M IDs. Authorizations with conditions (i.e., conditional ATOs) should be issued for a length of time sufficient to allow the conditions to be satisfied. Once the conditions are satisfied, a new unrestricted ATO will be granted for the remainder of the specific A&A process's ATO length.

m. Extension of a system's current ATO for a period not to exceed one year (365 days) may be requested only under one of the following conditions. The system must continue to maintain its complete set of A&A documentation (e.g., System Security Plan, Contingency Plan, POA&Ms). All actions to satisfy the following conditions must be completed within the extension period (i.e., no longer than 12 months).

(1) Transitioning to ongoing authorization;

(2) Planning for disposal;

(3) Consolidating into another system for its ATO. The scope of consolidation shall be approved by the OCISO prior to submitting the ATO extension request;

(4) Transitioning into a cloud environment for its ATO. The scope of the transition into the cloud environment shall be approved by the OCISO prior to submitting the ATO extension request;

(5) Re-competing the system's contract;

(6) Completing the upgrade/replacement of major infrastructure components;

(7) Completing the system's security assessment has been delayed due to contract issues; or

(8) Complying with Showstopper Controls as listed in CIO-IT Security-06-30.

n. An information system undergoing a three-year re-authorization having outstanding High or Very High/Critical vulnerabilities identified during its security assessment, may request a one-time extension for a period not to exceed 30 days from the date of the ATO expiration to allow mitigation of the High and Very High/Critical vulnerabilities. No more than two extensions may be granted under this condition.

4. Risk Assessment.

a. Every government and contractor IT system operated must undergo a security control assessment utilizing GSA test cases based on NIST SP 800-53, Revision 5, Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans, and the annual requirements provided by the OCISO.

b. All Internet accessible information systems and all FIPS 199 High impact information systems are required to complete an independent penetration test (or 'pentest') and provide a Penetration Test Report documenting the results of the exercise as part of the A&A package. In addition, these same systems must complete penetration tests annually. "Independent" testing means the testers are free from any perceived or actual conflicts of interest regarding the development, operation, or management of the information system(s) targeted by the penetration test.

c. Independent vulnerability testing including penetration testing and system or port scanning conducted by a third-party, such as the GAO and other external organizations, must be specifically authorized by the AO and supervised by the ISSM.

d. The OCISO must identify sources of cyber threat information (e.g., DHS CISA Cybersecurity Directives, US-Computer Emergency Readiness Team [US-CERT] Alerts, etc.) and a process for sharing the information, as appropriate.

e. The OCISO must create procedures to share common threats, vulnerabilities, and incident related information with the appropriate organizations.

f. Business impacts must be identified as part of the risk assessment process IAW GSA CIO-IT Security-06-30 and GSA CIO-IT Security-18-91.

g. Threats, vulnerabilities, likelihoods, and impacts must be appropriately identified and considered to assess cybersecurity, cyber supply chain risks, and/or privacy risks IAW GSA CIO-IT Security-06-30 and GSA CIO-IT Security-18-91.

h. All information systems must develop and maintain a POA&M IAW GSA CIO-IT Security-09-44. POA&Ms are the authoritative agency management tool for managing system risk and are used in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in agency programs and systems.

i. The Information Security Program Plan (ISPP), which documents the enterprise-wide common controls and hybrid controls with an enterprise-wide common portion, must be assessed at least every three years using GSA's security assessment process as defined in CIO-IT Security-06-30. A security assessment report will be produced based on this assessment.

5. Risk Management Strategy.

a. To implement and maintain a risk management process for all information systems, the OCISO is guided by NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View, NIST SP 800-30 Revision 1, Guide for Conducting Risk Assessments, GSA CIO-IT Security-06-30, GSA CIO-IT Security-18-90, GSA CIO-IT Security-18-91, and all identified A&A process procedural guides as required.

b. AOs and System Owners must follow the organizational risk tolerance as expressed in GSA CIO-IT Security-18-91.

c. The OCISO must update the organizational risk tolerance as expressed in GSA CIO-IT Security-18-91, on a biennial basis based on changes in GSA's risk posture and Federal guidance on any GSA critical infrastructure or sector risks.

6. Supply Chain Risk Management.

a. The OCISO Cyber Supply Chain Risk Management (C-SCRM) Program addresses cyber risks both prior to and post contract award for information and computer technology (ICT) products and services. Accordingly, all GSA systems must manage risks to their cyber supply chain IAW:

(1) CIO-IT Security-21-117, OCISO Cyber Supply Chain Risk Management (C-SCRM) Program;

(2) CIO-IT Security-22-120, Supply Chain Risk Management (SR) Controls;

(3) CIO-IT Security-09-48, Security Language for IT Acquisition Efforts; and

(4) NIST SP 800-161r1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations.

b. Cyber Supply Chain events must be reported to the GSA IT Service Desk IAW GSAM Case 2021-G511, Change 35.

c. Acquisition professionals must consider potential cyber supply chain risks as part of the acquisition process as follows:

(1) IAW GSAM Case 2021-G511, Change 35

(2) When applicable, if the original equipment manufacturer (OEM) has a program to authorize both the product's pricing and sale by a third-party vendor, proof of the bidder's authorized standing with the OEM is required prior to any business-award.

d. Systems and their suppliers and third-party suppliers must comply with Public Law 115-91, National Defense Authorization Act for Fiscal Year 2018, Section 1634, Prohibition on Use of Products and Services Developed or Provided by Kaspersky Lab, which prohibits the use of any hardware, software, or services developed or provided in whole or in part by— (1) Kaspersky Lab (or any successor entity), (2) any entity that controls, is controlled by, or is under common control with Kaspersky Lab, or (3) any entity of which Kaspersky Lab has majority ownership.

e. Systems, their suppliers, and third-party partners must comply with the Federal Acquisition Regulation (FAR) 52.204-25, Prohibition on Certain Telecommunications and Video Surveillance Services or Equipment, under Public Law 115-232, John S. McCain National Defense Authorization Act for Fiscal Year 2019, Section 889. This law prohibits the procuring or obtaining or extending or renewing a contract to procure or obtain equipment or services produced or provided by the following organizations unless an exception or waiver is granted per the law or the FAR:

- Huawei Technologies Company
- ZTE Corporation
- Hytera Communications Corporation
- Hangzhou Hikvision Digital Technology Company
- Dahua Technology Company
- Any subsidiary or affiliate of these five companies.

f. Appropriate personnel (e.g., Requiring Official, CO, COR) must assess a supplier's and third-party partner's supply chain prior to acquisition as part of contract requirements and as necessary thereafter. Assessments may consist of audits, tests, or other forms of evaluation as deemed necessary.

g. All information systems must develop anti-counterfeit procedures that include detection of counterfeit hardware or software components consistent with NIST SP 800-53, Revision 5.

CHAPTER 4: POLICY FOR PROTECT FUNCTION

This chapter provides security policy statements for the Protect function of the CSF. The Protect function allows GSA to develop and implement appropriate safeguards to ensure delivery of critical infrastructure services. The activities in the Protect function support the ability to limit or contain the impact of a potential cybersecurity event.

This chapter provides the specific policy statements supporting outcomes for the CSF Protect categories and subcategories. Appendix A details specific Protect category and subcategory definitions and unique identifiers.

1. Identity Management, Authentication and Access Control. The following GSA procedural guides provide specific implementation guidance and configuration settings/policies for GSA systems and organizations:

- GSA CIO-IT Security-01-01: Identification and Authentication (IA)
- GSA CIO-IT Security-01-07: Access Control (AC)
- GSA CIO-IT Security-03-23: Termination and Transfer
- GSA CIO-IT Security-07-35: Web Application Security
- GSA CIO-IT Security-10-50: Maintenance
- GSA CIO-IT Security-12-67: Securing Mobile Devices and Applications
- Hardening Guides: Multiple guides for configuring various technologies IAW with GSA required security settings

a. All identities and credentials must be managed and administered IAW the procedural guides listed above.

b. All users issued GFE laptops/workstations are required to log into the workstation using a GSA issued PIV credential. The following groups of users are exempt from this requirement:

(1) Federal employees on detail to GSA issued a PIV by their assigned Agency.

(2) Employees or contractors expected to be employed for less than 180 days and not issued a PIV.

(3) Any person with a disability prohibiting the use of a PIV card and laptop.

(4) Any user with a PIV that is lost, forgotten at home, or damaged in any way, may contact the IT Service Desk to request a temporary exception to the above requirement, not to exceed 45 days.

c. Information system accounts must be managed for all systems, including establishing, activating, modifying, reviewing, disabling, and removing accounts. Reviews and validations of all user accounts shall be completed annually to ensure the continued need for system access.

d. Disabling and removal of user accounts supporting account management processes, to include:

(1) Supervisors being responsible for coordinating and arranging system access termination for all departing or resigning personnel, both Federal employees and contractors.

(2) Account removal being initiated by a user's supervisor, COR, or through the review of information provided by the OCISO (e.g., separation lists, role revisions). Data and system owners must verify within 30 days that separated personnel no longer maintain access to GSA IT systems or resources.

(3) Termination and transfer procedures being incorporated into the authorization process for all information systems IAW GSA CIO-IT Security-03-23.

e. Request, including modifications, and approval routing in support of account management processes must ensure:

(1) All access requests require at least one supervisor approval. Access requests submitted directly from a user must not be accepted, regardless of position;

(2) Users complete and send access requests to their supervisor or COR, not directly to the data or system owner;

(3) Access requests are routed to the data or system owner by a user's supervisor, COR, ISSO, ISSM, director, or designated official.

f. Authorizations supporting the account management processes must assure:

(1) Supervisors are responsible for coordinating and arranging system access requests for all new or transferring users and for verifying an individual's need-to-know.

(2) Data owners/system owners, with assistance from the designated ISSO, must ensure system access is restricted to authorized users who meet GSA and system access requirements, are familiar with internal security practices, and have completed requisite security and privacy awareness training programs.

(3) System access authorizations must enforce job function alignment, separation of duties, and be based on the principle of need-to-know. Contractors with system access must utilize a gsa.gov email account to conduct business with GSA.

g. Data or system owners must grant access to the information system based on a valid need-to-know/need-to-share determined during the account authorization process and the intended system usage.

h. Orphaned accounts, i.e., a user account that has demonstrated, or is expected to demonstrate, an extensive period of idle time consistent with account abandonment, must be disabled.

i. GSA Affiliated Customer Accounts (GACAs) are a means where any gsa.gov user can share collaboratively in a secure environment with non-GSA users not normally provided a gsa.gov email account. Procedures for setting up a GACA account by an affiliated customer of GSA can be found at GSA IT's GACA Accounts webpage. GACA accounts are not to be used by GSA employees, contractors, or other users (detailees, interns, etc.) requiring regular/repeated access to the GSA network for GSA's Google domain to conduct business. For questions on the proper use of a GACA account or assistance in proper set up, please contact the local IT Manager or Regional ISSO.

j. System/network administrators must have separate administrator and user accounts, if applicable (e.g., Microsoft Windows accounts). The administrator privileged account must only be used when administrator rights are required to perform a job function. A normal user account should be used at all other times.

k. Termination and transfer procedures must be followed for all information systems IAW GSA CIO-IT Security-03-23.

l. Physical access to GSA assets must be managed and protected IAW GSA CIO-IT Security-12-64, Physical and Environmental Protection (PE). Facilities management offices may be heavily involved in implementing these controls, especially where controls are associated with multiple systems.

m. Physical and environmental security controls must be commensurate with the level of risk and must be sufficient to safeguard IT resources against possible loss, theft, destruction, accidental damage, hazardous conditions, fire, malicious actions, and natural disasters.

n. GSA servers, routers, and other communication hardware essential for maintaining the operability of GSA systems and their connectivity to the GSA Network, must be placed in an isolated, controlled-access location (i.e., behind locked doors).

o. Limit access to rooms, work areas/spaces, and facilities containing agency systems, networks, and data to authorized personnel. A list of current personnel with authorized access shall be maintained and reviewed annually to verify the need for continued access and authorization credentials.

p. Visitor access records shall be maintained for facilities containing information systems (except for those areas within the facility officially designated as publicly accessible). These records must be reviewed at least annually. Visitor access records include:

(1) Name and organization of the person visiting;

(2) Signature of the visitor;

(3) Form of identification;

(4) Date of access;

(5) Time of entry and departure;

(6) Purpose of visit;

(7) Name and organization of person visited; and

(8) Signature and name of the individual verifying the visitor's credentials.

q. Remote access connections, sessions, and timeout/termination parameters must meet the requirements specified in the procedural guides listed in Section 1 of this Chapter.

r. The following time frames regardless of user activity:

(1) Remote sessions must be terminated after 30 minutes of inactivity.

(2) Thirty days for systems at AAL1.

(3) Twelve hours for systems at AAL2 and AAL3.

s. An AO, upon concurrence of the GSA CISO, may grant a deviation to individual requirements specified in the guides only if the system is technically unable to implement the requirement or there is an approved business justification and sufficient compensating controls have been implemented to reduce the risk to an acceptable level. See Chapter 1, Section 5, Compliance and Deviations.

t. Remote access/endpoint security.

(1) All desktop or laptop computers, including personal devices, connecting remotely to GSA must have anti-virus software running with the latest signature files, a firewall installed and running, and all security patches installed. Failure to have current security signatures or patches may result in loss of access to the GSA network or data.

(2) All computers accessing GSA through a GSA Secure Sockets Layer (SSL) or Internet Protocol Security (IPsec) Virtual Private Network (VPN) must allow an endpoint device with the ability to check for the presence of a client firewall, up-to-date virus protection software and up-to-date patches. The endpoint device must also verify the absence of malicious software (e.g., Trojans, worms, malware, spyware, etc.) on the

client machine. Machines failing this scan will not be allowed access to the GSA network or any GSA IT resources.

(3) Only properly secured GSA GFE (based on the scans noted above) will be allowed unrestricted remote access to the GSA network.

(4) Personal computers and/or contractor computers will only be allowed access to the Citrix NetScaler and will not have the ability to map local drives (contingent on passing the scans noted above). No PII or other data deemed sensitive by the data owner shall be stored on non-GFE.

(5) In special cases for remote administration and maintenance tasks, contractors will be allowed restricted IPsec access to specific GSA IP addresses (contingent on passing the scans noted above).

u. Remote access to the GSA domain must be restricted to secure methods using approved identification and authentication methods to provide detection of intrusion attempts and protection against unauthorized access.

(1) Individuals other than GSA employees and contractor personnel are not allowed to use GSA furnished computers, a GSA VPN connection, or a GSA provided or funded internet connection.

(2) Split tunneling is not permitted when connected to the GSA network (no connections to other networks or computers). However, accessing GSA's network via the GSA-provided VPN software over a network is allowed.

(3) When using the GSA IT IPsec VPN, users must connect using only IP and must have the client firewall bound to all network adapters.

v. The AO or their designee must grant remote access (i.e., external to GSA's network), privileges only to those GSA employees and contractors with a legitimate need for such access as approved.

w. Access permissions and authorizations management must meet the parameter requirements specified in the procedural guides listed in Section 1 of this Chapter.

x. Workstations shall only be operated with assigned user level rights. If elevated privileges on a workstation are required as part of assigned job duties (such as development work), they must be exercised in an admin VDI pool virtual workstation.

y. User account privileges must be reviewed across the appropriate Service and Staff Office application portfolio to assess incompatible and non-compliant role assignments (e.g., review of user access assignments across multiple significant systems sharing data or passing transactions to identify conflicts with separation of duties policy).

z. All GSA systems must implement logical access controls to authorize or restrict the activities of users and system personnel to authorized transactions and functions IAW GSA CIO-IT Security-01-07.

aa. The delegation of user roles or permissions for applications, in particular those containing PII and/or other CUI, must be compliant with the principles of least privilege, separation of duties, and need-to-know.

bb. Privileged rights including but not limited to “administrator,” “root,” and “power user” shall be restricted to authorized employees and contractors as approved by the AO.

cc. Public users must be restricted to using designated public services.

dd. Information systems must enforce the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.

ee. User authorizations must be verified annually for all information systems to determine if they remain appropriate.

ff. Any access or permissions clearly violating established separation of duties policies must be coordinated with the designated SSO including Regional Offices ISSO to correct or resolve conflicting role assignments.

gg. Shared user accounts violate the principles of separation of duties and non-repudiation and must be detected and removed when discovered.

hh. Systems requiring users to maintain an active email account must suspend or revoke access for users whose email credentials are no longer valid.

ii. Separation of duties. The following requirements apply to FIPS 199 Moderate and High systems only:

(1) Responsibilities with a security impact must be shared among multiple staff by enforcing the concept of separation of duties, which requires that individuals do not have control of the entirety of a critical process;

(2) Define and implement detailed separation of duties policies for IT systems based on the specific processes, roles, permissions, and responsibilities of personnel involved in departmental business operations.

(3) Every SSO including Regional Offices, must consider how a separation of duties conflict can arise from shared access to applications and systems. Specifically, application programmers and configuration management personnel should not generally

have concurrent access to the development and production environment. Failure to segregate access to source code and production code increases the risk of unauthorized modifications to programs being implemented into production systems, introducing vulnerabilities and negatively impacting the integrity and availability of data generated and stored in the system.

(4) Document job descriptions and roles to accurately reflect the assigned duties, responsibilities, and separation of duties principles. By clearly documenting position responsibilities and functions, employees are positioned to better execute their duties IAW policy.

(5) Establish formal procedures to guide personnel in performing their duties, with identification of prohibited actions violating separation of duties.

(6) Duties shall be segregated among users, ensuring the following functions shall not generally be performed by a single individual:

(a) Data entry and verification of data. Any data entry or input process requiring a staff member to inspect, review, audit, or test the input to determine that the input meets certain requirements should not permit the same individual to both enter and verify the data. The objective is to eliminate self-certification or verification of data input or entry procedures. Note that this could be an automated or manual process and is not limited to financial transactions.

(b) Data entry and its reconciliation to output. Any data entry or input process requiring reconciliation or matching of transactions to identify discrepancies should not permit the same individual to both enter and reconcile data.

(c) Input of transactions for incompatible processing functions (e.g., input of vendor invoices and purchasing and receiving information).

(d) Data entry and supervisory authorization functions (e.g., authorizing a rejected transaction to continue processing exceeding some limit requiring a supervisor’s review and approval).

(7) Ensure proper separation of duties for GSA IT system maintenance, management, and development processes.

(8) Information systems must enforce separation of duties through assigned access authorizations.

(9) Since critical processes can span separate and distinct applications and systems, all SSOs including Regional Offices will take a macro view of existing roles to define and establish incompatibilities and separation of duties conflicts across an entire business process. This means examining roles spanning multiple IT systems or applications to uncover conflicts not immediately apparent (e.g., an individual has

permissions to create and/or modify vendor data in a General Ledger system and the ability to create invoices and purchase orders in an Accounts Payable system).

(10) All SSOs including Regional Offices must establish physical and logical access controls to enforce separation of duties policy and alignment with organizational and individual job responsibilities.

(11) Conduct annual assessments to review the effectiveness of control techniques, with an emphasis on activities unable to be controlled through logical, physical, or compensating controls. The reviews determine whether in-place control techniques are maintaining risks within acceptable levels (e.g., periodic risk assessments).

jj. All GSA workstations and mobile devices shall initiate a device lock after 15 minutes of inactivity. The device lock shall remain in effect until the user re-establishes access using appropriate identification and authentication.

kk. OAuth 2.0 is an industry standard protocol approved by GSA. It enables a gsa.gov user to grant access to their account or data in Google Apps to a relying party. It is used in a wide variety of services for user authentication. The following policies apply to the use of OAuth 2.0.

(1) GSA IT's OCISO shall monitor and restrict the integration of gsa.gov accounts with OAuth 2.0 to third-party services including but not limited to; websites, Software as a Service (SaaS), mobile applications, and Google Apps Scripts.

(2) Auth 2.0 Access Scopes are used to limit the authorization granted to the relying service by the gsa.gov user. The Access Scopes listed below present risk to gsa.gov accounts and data and are prohibited unless integrated with websites, mobile apps, and SaaS authorized to operate by GSA and/or included in the GSA IT Standards Profile.

(a) Access Inbox and Contacts Information. Allows view of email messages and settings.

(b) Access Personal Information. Allows management of user calendars.

(c) Act on Behalf of User. Allows view and modify but not deletion of user email.

(d) Full Data Access. Allows view and management of files and documents in connecting users Google Drive.

(e) Limited Access to Data and Files. Can be varied from access to a single file to allowing the app to view and manage its own configuration data in Google Drive.

(f) Manage Devices. Administrator's scope to view and manage mobile devices' metadata.

(g) Manage User Activity. Administrator's scope to view users on a domain; manage org units in a domain; view org units in a domain; view and manage provisioning of users in a domain; general domain Application Program Interface (API) operations include managing a domain's language, organization name, max number of users; current number of users.

(h) Other. Miscellaneous permissions. Restrictions are detailed in the system authorization letter.

(i) Payment Information. Read Google Wallet credentials from the production environment.

(j) Read-only Access to Data and Files. “Read-only Access” to data and files.

(k) Access Location Information. Google Map Data API - View Google Maps engine data; Google FIT: Location.

(3) The OAuth 2.0 Access Scopes listed below are authorized for integration with gsa.gov accounts with no restriction.

(a) Basic Info. View an email address; View basic information about an account, including name, public profile URL, photo, gender, birthdate, country, language, and time zone.

(b) Limited access to data and Files. Access Google+ features which are generally public.

(c) Other access scopes similar to those in (a) and (b) above providing access to publicly available information and do not conflict with prohibited access scopes.

ll. Google Apps Script is a JavaScript cloud scripting language that facilitates the automation of routine tasks across Google Apps and third-party services. All scripts are subject to GSA IT review to verify author; access scope; where the script resides (e.g., internal vs external); type of data accessed; and storage of accessed data.

(1) Internally developed scripts are implicitly allowed but require review by the OCISO and may be restricted from use pending the results of the OCISO review.

(2) Internally developed scripts shall follow the GSA naming convention. “GSA” immediately followed by an underscore “_” or single dash “-”, a 1 to 5 character S/SO official symbol designation of the script’s author, immediately followed by an underscore

"_" or single dash "-", and followed by a descriptive script name (e.g., "GSA_IS_Script Name").

(3) Externally developed scripts are prohibited but may be allowed following OCISO review and approval.

mm. Technologies with file-sharing functionality (e.g., peer-to-peer networking software) require review by the OCISO prior to use and may be approved if the file sharing functionality has been limited or disabled.

nn. Contingency Plan/Continuity of Operations Plan contact lists containing only a person's name and home phone number and kept on a password protected electronic device (other Government approved smartphone devices, laptop, USB drive) do not require written permission or encryption. Paper "cascade lists," limited to name and home phone number, maintained for the purpose of emergency employee accountability are permissible with the approval of those individuals listed. All paper and other media must be kept in a locked facility or an otherwise secure location when not in use.

oo. PII/CUI stored on network drives and/or in application databases must have proper restricted access controls (i.e., userid/account and password) and shall be made available only to those individuals with a valid need-to-know.

pp. System and/or data owners must verify that data extracts containing PII are handled IAW the GSA Rules of Behavior for Handling PII (CIO P 2180.2). PII must only be disclosed on a need-to-know basis within GSA and disposed of IAW the applicable records retention schedule.

qq. A GSA Guest Wireless Network has been established in the Regional and Central Office Buildings to allow non-GFE access only to the Internet and GSA resources available to the public (www.gsa.gov). It is intended to be a service for customers of the agency, as well as vendors performing official business on site.

(1) Guest wireless accounts are not ENT accounts.

(2) Guest wireless traffic will be subject to the same content filtering as traffic on the production network.

rr. All non-GFE/workstations connected to the GSA Wired Network shall only be allowed access to the Internet (i.e., guest network only, no access allowed to the GSA resources).

ss. All GFE/GSA Procured Workstations/Mobile devices such as phones, tablets, etc., should connect to the GSA Wireless Network which requires an ENT account to access, rather than the Guest Wireless Network. Connecting in this manner will provide access to GSA resources as well as the Internet, similar to the GSA Wired Network.

tt. OCISO must approve all requests for access through the GSA Firewall. Firewall change requests must follow the process outlined in GSA CIO-IT Security-06-31, Firewall Change Request. This includes changes to desktop firewall and intrusion prevention systems.

uu. OCISO will block access to all external sites deemed to be a security risk to GSA. Exceptions to this policy must be approved by the CISO.

vv. GSA has implemented a Bring Your Own Device policy in GSA CIO-IT Security-12-67, allowing users with an ENT account to connect a non-GSA procured Wireless device to the GSA Wireless Network to access GSA resources.

ww. All information systems allowing authentication of users for the purpose of conducting government business electronically (accessed via the Internet or via other external non-agency controlled networks, such as partner VPN) complete a Digital Identity Acceptance Statement IAW NIST SP 800-63-3.

xx. Systems with a NIST SP 800-63-3 AAL of 2 or above used by Federal employees or contractors must accept Federal PIV cards and verify them IAW NIST SP 800-63-3 series requirements.

yy. All GSA systems must incorporate a proper user identification and authentication methodology. Refer to the GSA CIO-IT Security-01-01 for additional details.

zz. User IDs shall be unique to each authorized user.

aaa. Authentication schemes for all systems and users must utilize MFA using two or more types of authentication factors. GSA systems with non-privileged users may integrate with GSA approved centralized authentication services using Security Assertion Markup Language (SAML 2.0) or OpenID Connect. The centralized authentication services will manage the multi-factor authentication options available to the users to allow for users to have accessible and secure options suited for their affiliation and interaction with the system. Multi-factor authentication options made available shall prefer smartcard based public key infrastructure and webauthn options for GSA non-privileged users. Multi-factor authentication options made available to GSA business or public users can include one-time passwords delivered via a mobile app or push notifications but shall offer choices for webauthn where feasible.

bbb. An authentication scheme using passwords as a credential must implement the following password policy requirements:

(1) Passwords for accounts used to access operating systems (workstations and servers) must:

(a) Contain a minimum of 16 characters;

(b) Have passwords changed when a password is compromised or forgotten; and

(c) Not have complexity requirements.

(2) Passwords for system/other accounts (e.g., user, service, application) must:

(a) Contain a minimum of 8 characters;

(b) Have passwords changed when a password is compromised or forgotten; and

(c) Require a combination of letters, numbers, and special characters if no password checking solution is used; or

(d) Have no complexity requirements, if a password checking solution to check a database of known bad passwords is used (e.g., checks for commonly used, expected, or compromised passwords; dictionary words; repetitive or sequential characters such as ‘aaaaaaaa,’ ‘1234abcd,’ ‘1qaz2wsx;’ or context sensitive words such as the username or a derivative).

(3) Passwords for all mobile devices such as GSA approved smartphones, iPads, and tablets must be a minimum of 6 characters. The six-character password requirement also applies to personal mobile devices accessing GSA data or systems.

(4) Passwords must not be stored in forms (i.e., Windows dialog boxes, web forms, etc.).

(5) All default passwords on network devices, databases, operating systems, installed software, etc. must be changed.

(6) Password distribution:

(a) Passwords must never be distributed via regular mail or interoffice mail.

(b) User IDs and passwords must never be distributed together.

(c) User IDs and passwords must be distributed via separate emails or channels (e.g., email, text, telephone).

(d) Passwords used for authentication (other than default or one time use passwords) must not be transmitted in the clear.

(7) Users must be authenticated before resetting or distributing a password.

(8) One time use passwords must expire in two minutes if based on a real-time clock.

(9) Password managers are permitted as long as they are listed on the GSA IT Standards List with a Status of Approved or Exception.

ccc. E-commerce and publicly accessible systems must incorporate identification and authentication mechanisms commensurate with their security risks and business needs and may differ from the security requirements set forth by this policy. In such cases the identification and authentication mechanisms must be approved by the AO in writing and concurred by the OCISO.

2. Awareness and Training. All GSA employees and contractors, as appropriate given their role, must adhere to training requirements in GSA CIO-IT Security-05-29: Security and Privacy Awareness and Role Based Training Program.

a. Failure to comply with annual awareness and specialized IT security training requirements will result in termination of access to the GSA enterprise and applications. AOs can terminate system accounts.

b. Obtaining access to GSA resources must constitute acknowledgment that monitoring activities may be conducted.

c. Users have no expectation of privacy on GSA IT systems. All activity on GSA IT systems is subject to monitoring.

d. All GSA IT systems must display an approved warning banner to all users attempting to access GSA's computer systems indicating the system is subject to monitoring.

e. GSA enterprise users must read and acknowledge GSA Order CIO 2104.1B CHGE 2, GSA IT General Rules of Behavior, within 90 days of being granted access to the enterprise, and annually thereafter.

f. All internal GSA IT systems must display an approved warning banner to all users attempting to access GSA's computer systems. The following warning banner must be based on these instructions:

(1) Paragraph two of the warning banner is only required if the system contains CUI;

(2) Paragraph three is optional but is a best practice.

(3) For publicly accessible sites (i.e., open to the Internet), the sentence "Therefore no expectation of privacy is to be assumed" shall be removed.

**********WARNING**********
This is a U.S. General Services Administration Federal Government computer system that is "FOR OFFICIAL USE ONLY." This system is subject to monitoring. Therefore, no expectation of privacy is to be assumed. Individuals found performing unauthorized activities may be subject to disciplinary action including criminal prosecution.

This system contains Controlled Unclassified Information (CUI). All individuals viewing, reproducing or disposing of this information are required to protect it in accordance with 32 CFR Part 2002 and GSA Order CIO 2103.2 CUI Policy.

For additional information: [contact information or website where users can get help]
****

g. Users of GSA IT resources must use only properly licensed software registered for GSA use. Users should consult with GSA IT if there is uncertainty about whether the licensing conforms to Government requirements.

h. Purchased software, and upgrades to existing software, must be able to run with user level rights. Existing software may be configured to allow for read/write access to a specific folder to allow it to function.

i. All GSA users must abide by software and digital media copyright laws and must not obtain, install, replicate, or use unlicensed software and digital media.

j. Users of GSA IT resources must obtain all software from GSA sources and must not download software from the Internet without prior permission from the appropriate ISSO, as downloading software from the Internet may introduce malicious software such as viruses/worms into the GSA network.

k. Users must not install any software or hardware without approval through the IT Standards process and the Chief Technology Officer.

l. Local support or Client Engineering will install all approved software.

m. Users must not acquire, possess, trade, or use hardware or software tools that could be employed to evaluate or compromise GSA resources unless authorized by the appropriate ISSO. Such tools may, for example, defeat software copy protection, discover passwords, identify security vulnerabilities, or decrypt encrypted files.

n. GSA provides access to email and social media for Government business. However, users may occasionally make personal use of email and social media involving minimal expense to the Government and does not interfere with Government business. Prior to establishing an official GSA social media presence, users must inform

the Office of Strategic Communication's (OSC) Enterprise Web Management (EWM) group which can monitor and assist with GSA branding and other aspects related to dealing with the public.

o. Users must not use email or social media for any activity or purpose involving classified data.

p. Users must avoid the following prohibited email and social media usages:

(1) Transmitting unsolicited commercial announcements or advertising material, unless approved by management in advance.

(2) Transmitting any libelous or defamatory material pertaining to GSA, the Federal Government, or any agency employee or official.

(3) Transmitting sexually explicit or offensive material, non-business related large attachments, chain letters, un-authorized mass mailings, or intentionally sending a virus/worm.

q. Personal use of Government IT systems for Internet access must be kept to a minimum and must not interfere with official system use or access.

r. Users must avoid prohibited Internet usages including:

(1) Unauthorized attempts to break into any computer, whether belonging to GSA or another organization.

(2) Browsing sexually explicit, gambling sites, or hate-based web sites (i.e., websites supporting hate groups or hate speech as their primary purpose).

(3) Using Internet access for personal gain (i.e., making use of GSA resources for commercial purposes or in support of for-profit activities such as running a private business).

(4) Theft of copyrighted or otherwise legally protected material, including copying without permission.

(5) Sending or posting sensitive material such as GSA building plans or financial information outside of the GSA network.

(6) Automatically forwarding email messages from GSA email addresses to any non-Federal email account(s) or address(es).

(7) Sending email messages including sensitive information, such as PII, as deemed by the Data Owner, without GSA-provided encryption. Certified encryption modules must be used IAW FIPS 140-3/140-2.

(8) Activities in violation of GSA Ethics Policies, including but not limited to promotional materials, solicitations, partisan political activities in violation of the Hatch Act, financial trading, or any other activity in contravention of Federal Government ethical guidance, policies, or regulations.

s. If PII needs to be emailed outside the GSA network, encryption is required. Instructions can be found on the GSA Privacy Act Program InSite page in the section "Documents for Download." An email will be blocked if Social Security Numbers are sent unencrypted.

t. GSA prohibits an employee or contractor supporting GSA from creating or sending information using a non-official GSA electronic messaging account (i.e., company or personal email account).

u. Additional guidance regarding GSA's policy on email is available in the following GSA Orders:

(1) 2160.2B CIO CHGE 3, GSA Electronic Messaging and Related Services,
(2) ADM 7800.11A, Personal Use of Agency Office Equipment,
(3) CIO 2140.4, Information Technology (IT) Solutions Life Cycle (SLC) Policy
(4) CIO P 2165.2 CHGE 1, GSA Telecommunications Policy.
(5) Guidance on social media is available in GSA Order OSC 2106.2.

v. GFE must not be taken on international travel without prior approval. Users must submit a GSA IT Service Desk ticket and receive approval from GSA IT and their supervisor with a recommendation for approval or disapproval from the OMA Threat Management Office related to country specific threat assessment.

(1) Covered Individuals, as defined in Security Executive Agency Directive (SEAD) 3, must contact OMA prior to any international travel.

(2) OMA will provide direction on foreign contact, security precautions, mobile devices, etc.

(3) Any GSA employee who must work while overseas (except for OIG employees) shall be issued loaner devices by GSA IT when traveling outside the United States, or any area deemed to have an elevated risk during the period of travel. The loaner devices must be returned to GSA IT immediately upon the employee's return. These loaner devices shall be wiped immediately by GSA IT to ensure no data remains resident on the system(s) issued.

(4) If access to the GSA network is needed when traveling outside the United States, use a GSA virtual interface (e.g., Citrix, VDI); connecting to the VPN is prohibited.

(5) Limit WiFi connections to trusted outlets (e.g., business office); do not use public WiFi.

(6) If taking a GFE phone, submit an IT Service Desk ticket for International Service. If the phone is connected to WiFi while overseas, it must be wiped upon return.

3. Data Security.

a. All PII/CUI and PCI data, and business sensitive data as determined by the AO, and authenticators, including but not limited to passwords, tokens, keys, certificates, and hashes must be encrypted everywhere (i.e., at file level, database level, at rest, and in transit). Encryption algorithms and modules must be FIPS 140-3/140-2 validated.

(1) For databases, encryption of the whole database, table, column, or field levels is acceptable, as appropriate. Other methods including, but not limited to, application encryption or tokenization is also acceptable.

(2) For web services connections, implement end-to-end encryption terminating the connection at the web server; connections terminated at a load balancer shall employ re-encryption techniques to ensure end-to-end encryption.

(3) Internet accessible Websites shall implement HTTPS Only with HTTP Strict Transport Security (HSTS), have no weak ciphers, have no weak protocols, and preload .gov domains.

b. Physically control and securely store information system media within controlled areas.

c. PII/CUI stored on network drives and/or in application databases must have proper access controls (i.e., user identification and authentication) and shall be made available only to those individuals with a valid need-to-know.

d. GSA provided portable storage devices (e.g., USB flash drives, SD cards, etc.) cannot be used on external systems (e.g., personal computers, other agency systems).

e. Web sites (internal and public) with logon functions, must implement Transport Layer Security (TLS) encryption with a FIPS 140-3/140-2 validated encryption module. SSL/TLS implementation must be IAW GSA CIO-IT Security-14-69, SSL/TLS Implementation Guide.

f. All sensitive information, such as PII/CUI, as deemed by the data owner, which is transmitted outside the GSA firewall, must be encrypted. Certified encryption modules must be used IAW FIPS 140-3/140-2.

g. An employee or contractor shall not physically take PII from GSA facilities (including GSA managed programs housed at contractor facilities under contract), or access remotely (i.e., from locations other than GSA facilities), without written permission from the employee's supervisor, the data owner, and the IT system AO. Approvals shall be filed with the employee's supervisor. This applies to electronic media (e.g., laptops, USB drives), paper, and any other media (e.g., CDs, DVDs) that may contain PII.

h. PII/CUI data may only be accessed remotely from GFE or through an approved GSA virtual interface (i.e., Citrix and/or VDI).

i. If PII/CUI needs to be emailed outside the GSA network encryption is required. Instructions can be found on the privacy web page in the section "Documents for Download." An email will be blocked from transmittal if Social Security Numbers are attempted to be sent unencrypted.

j. If PII/CUI needs to be sent by courier, printed, or faxed several steps should be taken. When sending PII/CUI by courier mark, "signature required" when sending documents. This creates a paper trail in the event items are misplaced or lost. Do not let PII documents sit on a printer where unauthorized employees or contractors can have access to the information. When faxing information, use a secure fax line. If one is not available, contact the office prior to faxing, so they know information is coming, and contact them after transmission to ensure they received it. For each event, the best course of action is to limit access to PII/CUI only to those individuals authorized to handle it, create a paper trail, and verify information reached its destination.

k. GSA information system assets must adhere to the guidance provided in GSA CIO-IT Security-01-05, GSA CIO-IT Security-06-32, and GSA CIO-IT Security-12-64 as assets are removed, transferred, or disposed of.

l. The availability and usability of GSA equipment and software must be maintained and safeguarded to enable agency objectives to be accomplished.

m. Systems containing permanent electronic records must be maintained in an electronic format IAW OMB M-19-21.

n. All permanent and temporary email records must be accessible electronically in an electronic format.

o. Data (including relevant and pertinent documentation), must be protected against unauthorized access, tampering, alteration, loss, and destruction during production, input, output, handling, and storage. This protection must include clarification for labeling sensitive security documentation IAW GSA policies. Additional guidance may be found in GSA CIO-IT Security-12-63, System and Information Integrity.

p. When using password generated encryption keys, a password of at least eight (8) characters with a combination of letters, numbers, and special characters is required.

q. Systems implementing encryption must follow the key management procedures and processes documented in GSA CIO-IT Security-09-43: Key Management.

r. Data integrity and validation controls must be used on all information systems requiring a high degree of integrity.

s. Ensure data integrity is protected IAW GSA CIO-IT Security-12-63.

t. Controls shall be put in place to monitor or detect changes or updates to systems outside the parameters of a system's baseline operating characteristics. This includes the ability to monitor resource usage and allocation.

u. The requirements for testing and development environments identified in GSA CIO-IT Security-01-05 must be met.

v. Hardware assets must be inspected upon receipt to ensure their authenticity.

w. After receipt, hardware assets must be protected against unauthorized access, tampering, alteration, loss, and destruction during production, input, output, handling, and storage.

x. Contractors shall return all GSA data when they no longer provide GSA contract support and at the end of their contract.

4. Information Protection Processes and Procedures.

a. All information systems must be securely configured IAW with GSA IT technical guides and standards, updated, and patched before being put into operation and while in operation.

b. GSA information systems, including vendor owned/operated systems on behalf of GSA, must configure their systems in agreement with GSA technical guidelines, NIST guidelines, DISA STIG guidelines (High Severity/CAT I), Center for Internet Security guidelines (Level 1), or industry best practice guidelines, as deemed appropriate. Any GSA security benchmark that has been published for a particular technology must be referenced to securely configure that technology. GSA security benchmark requirements must be implemented within (180) days of the benchmark's publication. GSA benchmarks may be exceeded but not lowered.

c. All new technology developments, designs, and implementations shall use industry best practices, Government guidelines, and Government audit findings as they become available.

d. GSA IT Security Policy must be incorporated into each phase of the system development lifecycle, (e.g., initiation, planning, development/acquisition, implementation, operation, and disposal), for all GSA information systems.

e. System owners must use GSA Order CIO 2140.4 as a guide when managing security throughout the system's life cycle.

f. Cloud-based system owners should use CIO-IT Security-19-102, OCISO DevSecOps Program, to fully integrate security with development and operations teams.

g. ISE must approve all Security Architecture designs prior to implementation.

h. Configuration changes must be controlled IAW the security controls and processes described in GSA CIO-IT Security-01-05.

i. Information system backups and testing of those backups must be accomplished IAW GSA CIO-IT Security-06-29.

j. Ensure all agency systems and networks are located in areas not in danger of water damage due to leakage from building plumbing lines, shut-off valves, and other similar equipment to support meeting federal and local building codes.

k. Install and ensure operability of fire suppression devices, such as fire extinguishers and sprinkler systems, and detection devices, such as smoke and water detectors, in all areas where agency information systems are maintained (this includes server rooms, tape libraries, and data centers) to meet federal and local building codes.

l. Install and ensure operability of air control devices, such as air-conditioners and humidity controls, in all areas where agency information systems are maintained (this includes server rooms, tape libraries, and data centers) to meet federal and local building codes.

m. The guidance provided in GSA CIO-IT Security-12-64 for a secure physical environment for information systems must be applied. Facilities management offices may be heavily involved in implementing these controls, especially where controls are associated with multiple systems.

n. All GSA data from information system media, both digital and non-digital, must be sanitized IAW methods described in GSA CIO-IT Security-06-32 before disposal or transfer outside of GSA.

o. The OCISO shall update this security policy and IT Security Procedural guides biennially, or more frequently as Federal or GSA guidance or the threats, vulnerabilities, or risks to GSA dictate.

p. HSSOs, for their FISMA reportable systems, shall track the performance measures/goals presented by the OCISO. AOs, system owners, ISSMs, and ISSOs shall support these measures. The CISO shall at least annually assess and report on the performance and goals.

q. All systems must adhere to the A&A processes in GSA CIO-IT Security 06-30, security requirements in this policy, and GSA IT Security Procedural guides. At a minimum, annual reviews and updates, when necessary, are required to reflect changes in Federal or GSA processes and guidance.

r. The OCISO will implement dashboards and reports, as appropriate, to provide stakeholders and management personnel with information on the security status of information systems and assets.

s. Contingency plans must be developed and revised annually, as necessary, for all IT systems IAW GSA CIO-IT Security-06-29. The plans must include recovery procedures, a separate disaster recovery plan may be developed if necessary.

t. Incident response plans must be developed and revised annually, as necessary, for all IT systems IAW GSA CIO-IT Security-01-02. The plans must include incident recovery processes, a separate incident recovery plan may be developed if necessary.

u. Contingency plans must be annually tested IAW GSA CIO-IT Security-06-29.

v. Incident response plans must be annually tested IAW GSA CIO-IT Security-01-02.

w. Background investigation requirements for access to GSA information systems (including contractor operations containing GSA information) shall comply with GSA Order ADM 2181.1, Homeland Security Presidential Directive-12 Personal Identity Verification and Credentialing, and Background Investigations for Contractors. Temporary contractors (work duration of 15 days or less) requiring access to IT systems (e.g., vendor/contractor summoned for an emergency service call) are not required to have a background investigation and require escort upon entry and while inside a GSA-controlled facility.

x. A favorable initial fitness/suitability determination must be granted, and a Tier 1 or higher background investigation initiated before access to the GSA network or any GSA IT system. There shall be no waivers to this requirement for GSA network and IT system access for GSA employees or contractors.

y. A favorable initial fitness/suitability determination must be granted, and a Tier 2 or higher background investigation initiated before access to PII/CUI is granted. The authority and access shall be determined by the appropriate GSA supervisor (for GSA employees) or CO (for contract personnel), data owner, and the system's AO. Each

system's AO, with the request of the GSA supervisor, data owner or CO, shall evaluate the risks associated with each such request.

z. A favorable suitability determination must be completed at a Tier 2 or higher background investigation before privileged access to the GSA network or IT systems is granted. A waiver may be requested to maintain GSA business operations; however, such requests should be used judiciously and not incur unnecessary risks to GSA.

aa. If final adjudication of a background investigation is unfavorable, GSA network and IT system access must be revoked, and any GFE, including the GSA PIV card, must be retrieved and returned to OMA.

bb. Vulnerabilities and weaknesses (system and program level) requiring mitigation must be managed using the processes described in GSA CIO-IT Security-09-44.

cc. The OCISO will review POA&Ms quarterly and provide system level and management reports IAW GSA CIO-IT Security-09-44.

5. Maintenance.

a. Maintenance and repair of organizational assets must be performed and recorded with approved tools IAW GSA CIO-IT Security-10-50.

b. Maintenance of agency hardware and software must be restricted to authorized personnel.

c. System administration and patch implementation must be restricted to authorized personnel.

d. Remote or non-local maintenance of organizational assets must be authorized, recorded, and authenticated via MFA IAW GSA CIO-IT Security-10-50.

6. Protective Technology.

a. The requirements for security auditing/logging capabilities and their review must be implemented on GSA systems IAW GSA CIO-IT Security-01-08, Audit and Accountability.

b. All systems must, upon request, provide logs to the Secretary of Homeland Security through the Director of CISA and to the FBI, consistent with applicable law and as required by EO 14028, Section 8(e).

c. Auditing of actions regarding PII stored on network drives and/or application databases must be captured (e.g., type of action, date/time, user, source of action, outcome of action).

d. Computer-readable data extracts from databases holding PII must be logged, including creator, date, type of information, and user.

e. Restrict access to information system media (e.g., disk drives, diskettes, internal and external hard drives, and portable devices), including backup media, removable media, and media containing sensitive information to authorized individuals.

f. Protect digital media during transport outside of controlled areas using a certified FIPS 140-3/140-2 encryption module; non-digital media shall follow GSA personnel security procedures.

g. Users must secure portable storage devices and removable media using the same policies and procedures as paper documents as prescribed by OHRM policies.

h. Users must protect portable storage devices and removable media in the same manner as a valuable personal item and should not leave them unattended in public places, automobiles, etc.

i. Information systems must run with the least amount of system privilege needed to perform a specific function and support system access granted on a need-to-know basis.

j. Information systems must be configured to the most restrictive mode (e.g., limiting ports, protocols, services, etc.) consistent with operational requirements.

k. Google Chrome Extensions (often developed by third parties) extend Google Chrome and Google Apps functionality. Extensions shall be disabled by default and enabled for business purposes following review and approval by OCISO Security Engineering Division.

l. The installation or use of unauthorized instant messaging (IM) software is prohibited (i.e., must use an approved GSA standard).

m. Bluetooth is approved for use on GSA GFE. The following restrictions apply:

(1) Devices must use the Bluetooth Protocol version 1.2 or later. If the device was manufactured 2005 or later, the version must be confirmed by consulting the device specifications.

(2) If a password/PIN must be chosen for device pairing the user should use a combination of letters and numbers when possible. A four digit pin should not be used unless this has been hard coded by the manufacturer. Users should also use a different passcode/PIN for each separate device pairing.

(3) The computer/device should not be discoverable except as needed for pairing. Discoverable mode (also known as "visible mode" or "pairing mode") allows the pairing of two Bluetooth devices. Users must ensure discoverable mode is disabled after pairing is completed.

(a) Bluetooth capabilities must be disabled when they are not in use.

(b) Two devices should not remain connected for more than 23 hours at a time, since the encryption keys can repeat after this.

(c) Encryption should always be enabled for Bluetooth connections (i.e., "Security Mode 1" does not enable encryption, and therefore should never be used).

n. Hacking tools are not to be used on GSA workstations without permission from OCISO, including password crackers, software that bypasses network controls (e.g., Tor), or hacking toolkits (e.g., Kali, Metasploit).

o. All network devices either owned, managed, maintain a connection to a GSA facility, and/or handle GSA data shall be strategically positioned behind a GSA firewall to provide analysis/correlation, management structure, and minimize threats presented by external attacks.

p. If GSA systems interconnect, they must connect using a secure methodology providing security commensurate with the acceptable level of risk as defined in the system security plan and limiting access only to the information needed by the other system IAW GSA CIO-IT Security-01-07 and GSA CIO-IT Security-06-30.

q. GSA users must secure mobile devices, like all enterprise devices, against a variety of threats. This includes handling PII/CUI. Included in the definition of ‘Mobile devices’ are smartphones and tablets. Excluded in the definition of mobile devices are laptops since the security controls for laptops are quite different from smartphones. Also excluded in the definition are basic cell phones due to the limited security options

available and their limited threat. GSA has outlined information on mobile devices at: https://sites.google.com/a/gsa.gov/mobileinfo/. GSA CIO-IT Security-12-67 is designated as the GSA policy on mobile devices and applications and provides specific information security requirements.

r. GSA's Mobile Device Management (MDM) solution ensures Government issued phones have appropriate security including; encryption, application controls, passwords usage, remote locking, remote wiping, and operating system protection.

s. Users must not connect to GSA resources without complying with the requirements which the Guide describes.

t. GSA CIO-IT Security-12-67 details the steps necessary to use a personally owned mobile device, which include:

(1) GSA will install MDM on the device and enforce control security settings, including password usage, encryption, and inactivity timeout.

(2) GSA will ensure that GSA can wipe the device clean if it is lost or stolen or after repeated unsuccessful attempts at logon.

(3) GSA will not support personally owned mobile devices.

(4) Users must agree to and sign a GSA Personal Device Usage Agreement and the GSA Rules of Behavior for Personally Owned Mobile Devices.

u. Systems shall be implemented per the enterprise architecture principles in GSA Order CIO 2110.4. The principles contained in GSA Order CIO 2110.4 are consistent with OMB Circular A-130 which establishes the framework for architecture to address security controls for components, applications, and systems.

(1) In addition to the principles set forth in GSA Order CIO 2110.4, architecture practices cited in OMB's Federal Segment Architecture Methodology must be used during planning a new system or significant capability enhancement.

(2) GSA OCISO has determined that the implementation of enterprise architecture principles is provided as a common control by the Office of Enterprise Planning and Governance (IDR). For additional details, please refer to GSA CIO-IT Security-18-90.

CHAPTER 5: POLICY FOR DETECT FUNCTION

This chapter provides security policy statements for the Detect function of the CSF. The Detect Function allows GSA to develop and implement appropriate activities to identify the occurrence of a cybersecurity event. The activities in the Detect Function enable timely discovery of cybersecurity events.

The following paragraphs provide the specific policy statements supporting outcomes for the CSF Detect categories and subcategories. Appendix A details specific Detect category and subcategory definitions and unique identifiers.

1. Anomalies and Events.

a. GSA uses centralized MDM to manage the configuration and security of mobile devices. GSA provisions and activates MDM on each mobile device before issuing Government devices to users.

b. The OCISO ELP will be used to establish a baseline of activity for GSA systems/sensors on the network.

c. The OCISO will regularly review/analyze data provided with the ELP for indications of inappropriate or unusual activity. Suspicious activity or suspected violations must be investigated. Any findings must be reported to appropriate officials IAW GSA CIO-IT Security-01-02.

d. Information systems must produce audit/log records containing sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events.

e. The OCISO ELP will be used for the collection and correlation from GSA systems/sensors.

f. The GSA Incident Response Team will determine the impact of events (potential incidents and actual incidents) based on Federal and GSA guidance as described in GSA CIO-IT Security-01-02.

g. Personnel making the determination of whether a major incident has occurred (requiring Congressional reporting) will be conducted by the GSA Full Response Team as defined in GSA Order CIO 9297.2C CHGE 1, Information Breach Notification Policy, and requires at least the following members:

(1) GSA CIO;

(2) GSA CISO, leads the team for major non-privacy incidents;

(3) Mission or system owners;

(4) SAOP leads the team for major privacy incidents;

(5) Representative from the Office of General Counsel;

(6) Representatives from the OSC and the Office of Congressional and Intergovernmental Affairs, for awareness and coordination purposes only, and

(7) Security Engineering Division Director or representative.

h. GSA systems and the GSA Incident Response Team will adhere to Federal Laws and requirements associated with responding to cybersecurity vulnerabilities and incidents and GSA guidance as documented in GSA CIO-IT Security-01-02.

2. Security Continuous Monitoring.

a. OCISO will implement continuous monitoring of systems using Continuous Diagnostics and Mediation and other enterprise security tools as described in GSA CIO-IT Security-12-66, Information Security Continuous Monitoring.

b. Intrusion detection/protection systems must be implemented.

c. GSA organizations must define procedures to periodically monitor mobile device security to verify compliance with GSA requirements.

d. Monitoring procedures must include specific steps to be taken and protocol to be applied when reviewing audit/log data.

e. The OCISO must be informed in the event of an audit processing failure, and system personnel must take one of the following additional actions: shut down the information system, overwrite the oldest audit records, or stop generating audit records.

f. Access to physical spaces containing GSA IT assets must be monitored for unauthorized access and suspicious incidents IAW GSA CIO-IT Security-12-64.

g. Limit access to rooms, work areas/spaces, and facilities containing agency systems, networks, and data to authorized personnel. A list of current personnel with authorized access shall be maintained and reviewed annually to verify the need for continued access and authorization credentials.

h. Visitor access records shall be maintained for facilities containing information systems (except for those areas within the facility officially designated as publicly accessible). Visitor access records include:

(1) Name and organization of the person visiting;

(2) Signature of the visitor;

(3) Form of identification;

(4) Date of access;

(5) Time of entry and departure;

(6) Purpose of visit;

(7) Name and organization of person visited, and

(8) Signature and name of the individual verifying the visitor's credentials.

Visitor access records shall be reviewed at least annually.

i. Personnel activity will be monitored IAW GSA CIO-IT Security-01-08.

j. User activity will be monitored for indications of fraud, misconduct, or other irregularities.

k. All information systems must have up-to-date, agency-authorized virus protection software. Note that the use of Kaspersky Lab virus protection software, to include software embedded or integrated into third-party technology, is expressly prohibited.

l. All information systems must implement and enforce a malicious code protection program designed to minimize the risk of introducing malicious code (e.g., viruses, worms, spyware, Trojan horses) into agency systems and networks.

m. GSA monitors mobile device activity for unauthorized code, including mobile code, using MDM policies and rules of behavior as outlined at: https://sites.google.com/a/gsa.gov/mobileinfo/.

n. AOs and OCISO will ensure external service providers are connected via the Trusted Internet Connection, permitting monitoring and detection of events.

o. External service provider personnel who connect remotely to the GSA network must do so as described in Chapter 4, Section 1.v, regarding remote access and endpoint security, and must permit monitoring and detection of events.

p. For contractors and outsourced operations, implement appropriate safeguards to monitor GSA information and information systems for unauthorized access throughout all phases of a contract. Review contracts to ensure information security is appropriately addressed in the contracting language. GSA CIO-IT Security-09-48 establishes the language for GSA IT acquisitions contracts. All applicable NIST SP 800-53, Revision 5 controls should be put on contract (and a reasonable subset continuously monitored using guidance provided by the OCISO) for all contractor and outsourced operations.

Given that the GSA IT security program is risk-based, the system owner/program manager and ISSO can make risk-based decisions on tailoring the system's baseline security controls and then obtain concurrence from the AO and the CISO. Any controls tailored out of the baseline must have the rationale for the decision documented in the system's SSP.

q. Contractor Information systems must follow the monitoring requirements IAW External Information System Monitoring CIO 19-101 Rev1.

r. Monitoring will be performed as described IAW GSA CIO-IT Security-01-08.

s. GSA SSOs shall scan for unauthorized wireless access points quarterly and take appropriate action if such an access point is discovered.

t. Systems will be scanned for vulnerabilities of operating systems and web applications periodically IAW GSA CIO-IT Security-17-80. Vulnerabilities identified must be remediated IAW GSA CIO-IT Security-06-30.

u. ISSO checklists in GSA's Archer GRC will be completed by ISSOs and monitored by ISSMs to track the completion of recurring security tasks.

3. Detection Processes.

a. The OCISO must define the roles and responsibilities for detection personnel to ensure they understand and perform their assigned actions.

b. Systems must comply with Federal and GSA detection and monitoring requirements as specified in NIST SP 800-53, Revision 5 and IAW GSA CIO-IT Security-01-08.

c. OCISO detection personnel must ensure detected event information is communicated to appropriate personnel.

d. Detection process testing should be included during annual incident response testing.

e. The OCISO must review and update detection processes annually or when significant changes occur or problems are encountered with detection activities.

CHAPTER 6: POLICY FOR RESPOND FUNCTION

This chapter provides security policy statements for the Respond Function of the CSF. The Respond Function allows GSA to develop and implement appropriate activities to take action regarding a detected cybersecurity incident. The activities in the Respond Function support the ability to contain the impact of a potential cybersecurity incident.

The following paragraphs provide the specific policy statements supporting outcomes for the CSF Respond categories and subcategories. Appendix A details specific Respond category and subcategory definitions and unique identifiers.

1. Response Planning.

a. All information systems must have their contingency plans and incident response plans tested annually.

b. Lessons learned during contingency plan and incident response plan tests must be incorporated into revised plans.

2. Communications.

a. GSA employees and contractors on the Incident Response Team identified in GSA CIO-IT Security-01-02 are trained on their roles and responsibilities within 60 days of assignment and annually thereafter.

b. Personnel with contingency planning responsibilities must be trained in their contingency roles and responsibilities with respect to the information system annually.

c. Users must immediately report suspected vulnerabilities, security violations, and security incidents to the GSA IT Service Desk.

d. Users must immediately report lost or stolen portable storage devices to the GSA IT Service Desk.

e. All incidents involving the loss or theft of GSA hardware, software, and/or information in physical form must be reported immediately to the GSA IT Service Desk.

(1) Users must also report all losses to the Federal Protective Service via the appropriate Regional Hotline, as directed by the appropriate ISSO or the GSA IT Service Desk.

(2) Users must also report any loss occurring outside of Federal facilities to the local police.

(3) Lost PIV cards must be reported to the Central or Regional OMA office after reporting to the GSA IT Service Desk.

f. GSA Incident Response Teams must report incidents as described in GSA CIO-IT Security-01-02. FISMA requires “major incidents” to be reported to the U.S. Congress within seven days of detection.

g. Data breaches (i.e., loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users with an authorized purpose have access or potential access to PII, whether physical or electronic) shall also follow reporting and response procedures as defined in GSA Order CIO 9297.2C CHGE 1.

h. ISSOs must report any security incidents reported to them to the GSA IT Service Desk and GSA OCISO.

i. Information will be shared by the GSA Incident Response Team, as appropriate, and IAW GSA CIO-IT Security-01-02.

j. Coordination with stakeholders will be conducted by the GSA Incident Response Team, as appropriate, and IAW GSA CIO-IT Security-01-02.

k. Information sharing with external stakeholders will be conducted by the GSA Incident Response Team, as appropriate and in coordination with the GSA CISO, IAW GSA CIO-IT Security-01-02.

3. Analysis.

a. The OCISO will communicate notifications/alerts from detection systems for investigation by GSA’s Incident Response Team via email or the GSA IT Service Desk. Procedures must be documented for responses to detected irregularities.

b. The GSA Incident Response Team will investigate notifications/alerts from detection systems IAW GSA CIO-IT Security-01-02.

c. The GSA Incident Response Team will determine the impact of an incident in coordination with other personnel/organization, as appropriate, during the investigation process defined in GSA CIO-IT Security-01-02.

d. The GSA Incident Response Team will perform forensics analysis of incidents/the evidence of incidents, as necessary, to support investigations as described in GSA CIO-IT Security-01-02.

e. The GSA OCISO and Incident Response Team will categorize incidents IAW GSA CIO-IT Security-01-02.

f. The OCISO will establish a vulnerability management process for identifying vulnerabilities via internal testing/scanning.

g. The OCISO will notify personnel with security responsibilities of vulnerabilities disclosed via SAAs or other external sources.

h. ISSMs and ISSOs must report on the status of the SAAs to the Office of the CISO upon request.

4. Mitigation.

a. The GSA Incident Response Team, in coordination with system personnel, will contain incidents IAW GSA CIO-IT Security-01-02.

b. Incidents will be mitigated or remediated based on activities executed by the GSA Incident Response Team and system personnel, as described in GSA CIO-IT Security-01-02 and the system's recovery plan.

c. IAW GSA CIO-IT Security-06-30, system vulnerabilities must be:

(1) Remediated or mitigated IAW specified timeframes;

(2) Included in a Plan of Action and Milestones; or

(3) Included in an Acceptance of Risk Letter.

d. Systems must comply with the required actions specified in DHS Cybersecurity Directives. The OCISO Security Operations Division (ISO) collaborates with system personnel regarding directives and reports status to DHS, as required.

5. Improvements.

a. Incident response plans must be updated based on lessons learned during incident response or plan testing.

b. Contingency plans must be updated based on lessons learned during responses to disasters, other events invoking the contingency plan or plan testing.

c. Incident response strategies must be reviewed and updated, if necessary, at least annually to address system/organizational changes and problems or issues encountered while responding to incidents or plan testing.

CHAPTER 7: POLICY FOR RECOVER FUNCTION

This chapter provides security policy statements for the Recover Function of the CSF. The Recover Function allows GSA to develop and implement appropriate activities to maintain plans for resilience and to restore any impaired capabilities or services resulting from a cybersecurity incident. The activities in the Recover Function support timely recovery to normal operations to reduce the impact from a cybersecurity incident.

The following paragraphs provide the specific policy statements supporting outcomes for the CSF Recover categories and subcategories. Appendix A details specific Recover category and subcategory definitions and unique identifiers.

1. Recovery Planning. As part of a system's contingency planning process, recovery plans are exercised as part of a cybersecurity incident response or after the response, as appropriate.

2. Improvements.

a. As part of a system's contingency planning processes, lessons learned from contingency plan tests regarding recovery must be incorporated into a revised contingency plan.

b. As part of the system's contingency plan testing and incident responses or incident response plan testing, any lessons learned regarding recovery strategies will be updated in the appropriate plan.

3. Communications.

a. The GSA OCISO will coordinate with the OSC to determine the necessity, appropriate process, and means for managing public information regarding an incident.

b. The GSA OCISO will coordinate with the OSC to determine the necessity, appropriate process, and means for repairing GSA's reputation after an incident.

c. Recovery activities are communicated by the GSA Incident Response Team and system personnel, as appropriate and in coordination with the GSA CISO, IAW GSA CIO-IT Security-01-02 and the system's recovery plan.

APPENDIX A: CSF CATEGORIES/SUBCATEGORIES

The table below provides a listing of CSF categories and subcategories (including unique identifiers) and descriptions from the NIST CSF. Additional information is available in CSF Version 1.1.

Category/Subcategory
Function: Identify
Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.
ID.AM-1: Physical devices and systems within the organization are inventoried
ID.AM-2: Software platforms and applications within the organization are inventoried
ID.AM-3: Organizational communication and data flows are mapped
ID.AM-4: External information systems are catalogued
ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value
ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established
Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.
ID.BE-1: The organization's role in the supply chain is identified and communicated
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated
ID.BE-4: Dependencies and critical functions for delivery of critical services are established
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g., under duress/attack, during recovery, normal operations)
Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.
ID.GV-1: Organizational cybersecurity policy is established and communicated
ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners
ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed
ID.GV-4: Governance and risk management processes address cybersecurity risks
Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.
ID.RA-1: Asset vulnerabilities are identified and documented
ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources
ID.RA-3: Threats, both internal and external, are identified and documented
ID.RA-4: Potential business impacts and likelihoods are identified
ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk

Category/Subcategory
ID.RA-6: Risk responses are identified and prioritized
Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.
ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders
ID.RM-2: Organizational risk tolerance is determined and clearly expressed
ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis
Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.
ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholder
ID.SC-2: Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process
ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan
ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations
ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers
Function: Protect
Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.
PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes
PR.AC-2: Physical access to assets is managed and protected
PR.AC-3: Remote access is managed
PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties
PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)
PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions
PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multifactor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)
Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity related duties and responsibilities consistent with related policies, procedures, and agreements.
PR.AT-1: All users are informed and trained
PR.AT-2: Privileged users understand their roles and responsibilities
PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities
PR.AT-4: Senior executives understand their roles and responsibilities

Category/Subcategory
PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities
Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
PR.DS-1: Data-at-rest is protected
PR.DS-2: Data-in-transit is protected
PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition
PR.DS-4: Adequate capacity to ensure availability is maintained
PR.DS-5: Protections against data leaks are implemented
PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity
PR.DS-7: The development and testing environment(s) are separate from the production environment
PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity
Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.
PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g., concept of least functionality)
PR.IP-2: A System Development Life Cycle to manage systems is implemented
PR.IP-3: Configuration change control processes are in place
PR.IP-4: Backups of information are conducted, maintained, and tested
PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met
PR.IP-6: Data is destroyed according to policy
PR.IP-7: Protection processes are improved
PR.IP-8: Effectiveness of protection technologies is shared
PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed
PR.IP-10: Response and recovery plans are tested
PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)
PR.IP-12: A vulnerability management plan is developed and implemented
Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.
PR.MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools
PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access
Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.
PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy
PR.PT-2: Removable media is protected and its use restricted according to policy

Category/Subcategory
PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities
PR.PT-4: Communications and control networks are protected
PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations
Function: Detect
Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.
DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed
DE.AE-2: Detected events are analyzed to understand attack targets and methods
DE.AE-3: Event data are collected and correlated from multiple sources and sensors
DE.AE-4: Impact of events is determined
DE.AE-5: Incident alert thresholds are established
Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.
DE.CM-1: The network is monitored to detect potential cybersecurity events
DE.CM-2: The physical environment is monitored to detect potential cybersecurity events
DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events
DE.CM-4: Malicious code is detected
DE.CM-5: Unauthorized mobile code is detected
DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events
DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed
DE.CM-8: Vulnerability scans are performed
Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.
DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability
DE.DP-2: Detection activities comply with all applicable requirements
DE.DP-3: Detection processes are tested
DE.DP-4: Event detection information is communicated
DE.DP-5: Detection processes are continuously improved
Function: Respond
Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.
RS.RP-1: Response plan is executed during or after an incident
Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g., external support from law enforcement agencies).
RS.CO-1: Personnel know their roles and order of operations when a response is needed
RS.CO-2: Incidents are reported consistent with established criteria
RS.CO-3: Information is shared consistent with response plans
RS.CO-4: Coordination with stakeholders occurs consistent with response plans
RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness
Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.
RS.AN-1: Notifications from detection systems are investigated

Category/Subcategory
RS.AN-2: The impact of the incident is understood
RS.AN-3: Forensics are performed
RS.AN-4: Incidents are categorized consistent with response plans
RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g., internal testing, security bulletins, or security researchers)
Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.
RS.MI-1: Incidents are contained
RS.MI-2: Incidents are mitigated
RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks
Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.
RS.IM-1: Response plans incorporate lessons learned
RS.IM-2: Response strategies are updated
Function: Recover
Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.
RC.RP-1: Recovery plan is executed during or after a cybersecurity incident
Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.
RC.IM-1: Recovery plans incorporate lessons learned
RC.IM-2: Recovery strategies are updated
Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g., coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).
RC.CO-1: Public relations are managed
RC.CO-2: Reputation is repaired after an incident
RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams