GSA’s Approach to Identifying Requirements: FISMA, FedRAMP or Controlled Unclassified Information

February 15, 2022

Agenda

- 01 BLUF
- 02 What's the Problem
- 03 NIST-171 vs FedRAMP Qualifying Template
- 04 GSA Non-Federal Security & Privacy Review Process using NIST-171

BLUF

- Federal Law and GSA policy requires adherence to FISMA (Federal Information Security Modernization Act) requiring Assessment and Authorization (A&A) of Information systems resulting in an Authorization to Operate (ATO). FISMA applies to Federal Data regardless of environment of operation, on-prem or cloud, and Government/contractor.
  - Cloud XaaS systems are required to adhere to FedRAMP.
  - **Federal information systems** developed for or on behalf of Government (regardless of environment) are required to complete A&A based on the FIPS 199 Impact level of the system, resulting in an ATO.
- There are vendor solution(s) that are neither Federal Information Systems nor generally delivered as as Service via cloud requiring FedRAMP. GSA is piloting use of NIST 171 for Non-Federal Systems with additional safeguards to mitigate Supply Chain and Privacy risk.
- Framework for security review/usage of Non-Federal systems
  - Focused on protecting the confidentiality of controlled unclassified information (CUI) when the information is resident in nonfederal systems and organizations
  - Security and Privacy requirements are aligned to NIST 171, NIST 172, and select NIST 800-53 control measures, as applicable.
  - Result in development of an System Security Plan, Independent Assessment, and Plan of Action and Milestones to be used by GSA to inform a risk-based usage consideration. Does not result in a traditional ATO.
  - Process applicability requires GSA CISO AND Privacy Officer approval.
- Additional C-SCRM Requirements. Vendors must agree to participation in GSA C-SCRM Program including monitoring via third-party vendor risk illumination tools (e.g. Interos and BitSight), and completing and submitting Supplier Questionnaire and SCRM Plan.

Security and Privacy Requirements for Non-Federal Information Systems

- Scope and Applicability
  - For protecting the confidentiality of CUI when the information is resident in nonfederal systems and organizations;
  - when 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; **and**
  - 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.

- The requirements apply only to the components of nonfederal systems and organizations that process, store, and/or transmit CUI, or that provide protection for such components.

- The security requirements are intended for use by federal agencies in contractual vehicles or other agreements established between those agencies and non-Federal organizations.

- It does not change the requirements set forth in FISMA, nor does it alter the responsibility of federal agencies to comply with the full provisions of the statute, the policies established by OMB, and the supporting security standards and guidelines developed by NIST.

- The requirements are derived from FIPS-199, FIPS-200 and the NIST 800-53 Moderate security control baseline.

What's the problem?

Increased reliance on external service providers

Interaction with providers is increasingly Data driven

Provider's systems **may not** be federal info systems

Nonfederal systems **not subject** to FISMA or OMB A-130

If federal info provided is **CUI, must be protected** in nonfederal systems

SP 800-171 protects confidentiality of CUI on nonfederal systems

Who needs to comply with NIST 800-171?

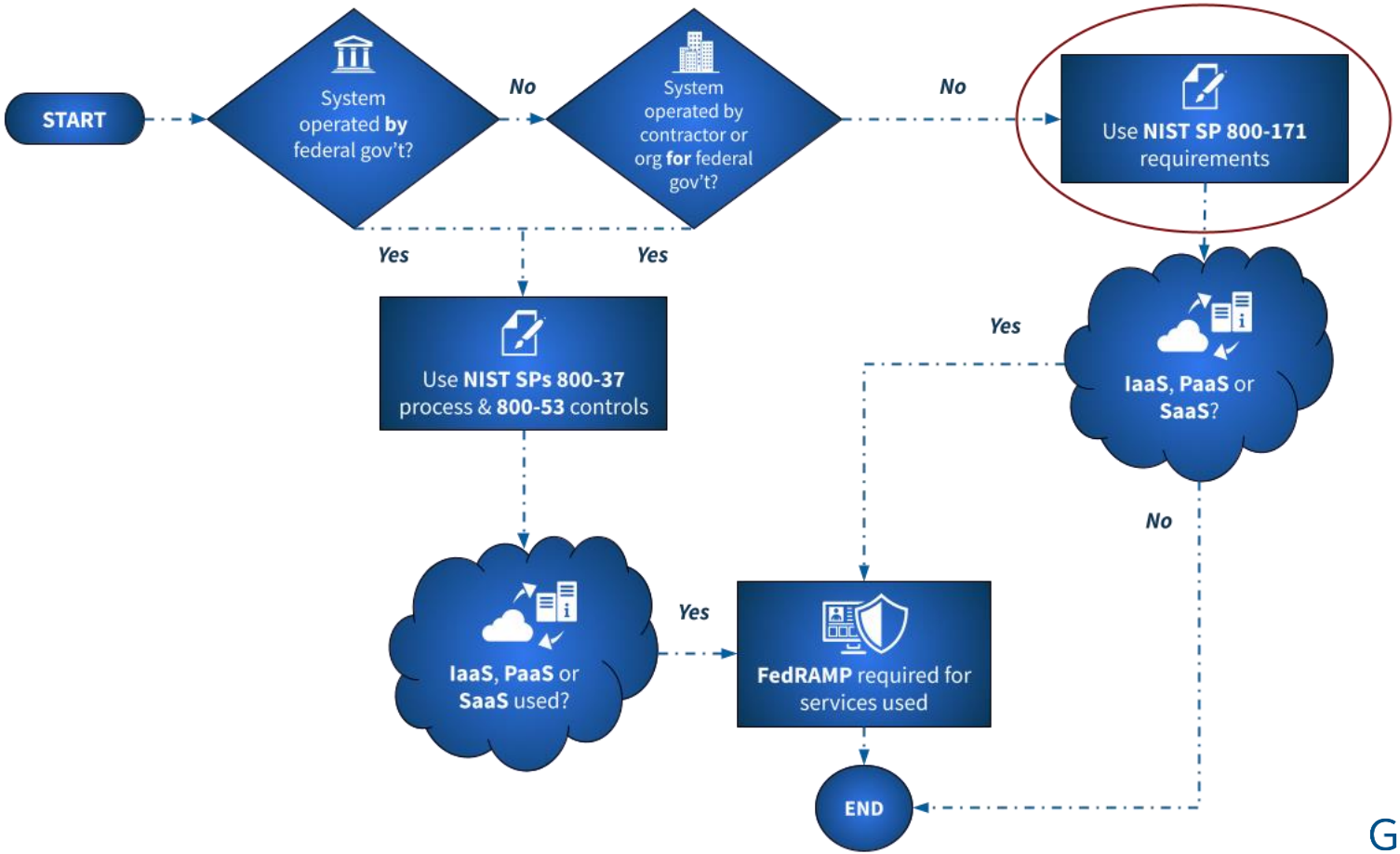
- Non-Federal entities that create, process, store or transmit **gov't CUI**

- Only applicable if mandated by **contract, grant or other agreement**

- Typical entities with **commodity** services

- Many service providers may have CUI **on premise** or in **cloud/provider based** systems & apps

Is NIST 800-171 Applicable?



GSA IT

What are Security and Privacy Requirements?

800-171 requires 110 controls in the following areas

3.1 Access Control
3.2 Awareness and Training
3.3 Audit and Accountability
3.4 Configuration Management
3.5 Identification and Authentication
3.6 Incident Response
3.7 Maintenance
3.8 Media Protection
3.9 Personnel Security
3.10 Physical Security
3.11 Risk Assessment
3.12 Security Assessment
3.13 System and Communications Protection
3.14 System and Information Integrity

800-172 requires 35 additional **conditional** controls in the following areas

3.1 Access Control
3.2 Awareness and Training
3.4 Configuration Management
3.5 Identification and Authentication
3.6 Incident Response
3.9 Personnel Security
3.11 Risk Assessment
3.14 System and Information Integrity
3.12 Security Assessment
3.13 System and Communications Protection
3.14 System and Information Integrity

GSA Privacy Officer required 13 additional **conditional** NIST SP 800-53 controls

AR-2 Privacy Impact and Risk Assessment
AR-3 Privacy Requirements for Contractors and Service Providers
AR-5(a) Privacy Awareness and Training
AR-7 Privacy-Enhanced System Design and Development
DI-1 Data Quality
DM-1 Minimization of Personally Identifiable Information
DM-3 Minimization of PII used in Testing, Training and Research
IP-1 Consent
IP-2(a) Individual Access
IP-4 Complaint Management
TR-1 Privacy Notice
UL-1 Internal Use
UL-2(a), (c), (d) Information Sharing with Third Parties

GSA Vendor Risk Assessment Program (VRAP) - GSA C-SCRM Requirements

SCRM Plan completed in agreement with NIST 800-161
SCRM Supplier Questionnaire
C-SCRM Risk Illumination - Vendors will be subject to risk assessment tool reviews

NIST 171 v FedRAMP Qualifying Template

NIST 171 v FedRAMP Qualifying Template

Section 2 - Service Questions	Response	Definitio
Do you Provide A Commodity Service		An informat… vided by a commercial service provider typically to a large and diverse set of consumers. The organization acquiring and/or receiving the commodit… structure and operations of the provider, and while the organization may be able to negotiate service-level agreements, the organization is typicall… fic security controls.
CUI information is resident in the System (CUI data) (https://www.archives.gov/cui/registry/category-list)		A categ… does not meet the standards for National Security Classification under Executive Order 12958, as amended, but is (i) pertinent to the national interests o… outside the federal government, and (ii) under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed lim… storage or dissemination.
Section 3 - FedRAMP Applicability Per OMB FedRAMP Policy Applicability Requirements		
Section 3.a Cloud Services		
Do you provide commercial or non-commercial cloud services (see section 3.c) that are provided by information systems that support the operations and assets of the departments and agencies, including systems provided or managed by other departments or agencies, contractors, or other sources.		(To be co…
Section 3.b.1- Essential Characteristics of Cloud Computing		
On-demand self-service		A consumer can unilaterally provision computing c… s, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.
Broad network access		Capabilities are available over the network and… rough standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations). server time and network stor… automatically without requiring human interaction with each service provider.
Resource pooling		The provider's computing resources are p… ltiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and assigned according to consumer demand. There is a sense of location i… the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, sta… mples of resources include storage, processing, memory, and network bandwidth.
Rapid elasticity		Capabilities can be elastically pro… bilities available for provisioning often appear to be…
Measured service		Cloud systems automatically… rocessing, bandwidth, and active user accounts). Re…
Section 3.b.2 Utilizes a Cloud Deployment Model meeting conditions of 3.b.1		
Private Cloud		The cloud infra… y the organization, a third party, or some com…
Community Cloud		The cloud infra… , policy, and compliance considerations). … off premises.
Public Cloud		The cloud infrastruc… combination of them. It exists on the premises of the…
Hybrid Cloud		The cloud infrastructure … rdized or proprietary technology that enables dat…
N/A On-Premise not meeting 3.b.1 requirements		On-premise deployment on infra…
Sec 3.c Cloud Service Models - Is the service offered as-a-service (e.g., Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS) as defined by NIST.		
IaaS		The capability provided to the consumer is to provis… cessing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The cons… does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking component… e.g., host firewalls).
PaaS		The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
SaaS		The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
N/A Cloud Hosted Shared Application not delivered "As a Service"		May be applicable if any "Essential Characteristics of Cloud Computing" identified in section 3.b.1 above are answered no. This implies the cloud application is not delivered "As A Service". As an example, if the vendor application is required to facilitate delivery of non IT services to GSA. Or the vendor application is secondary to the business service being provided.

General Outline of service

Section 3.a completed by GSA based on Section 3.b responses

Section 3.b evaluates service against NIST 800-145 cloud definitions

GSA IT

NIST 171 v FedRAMP Qualifying Template - Section 2

Section 2 - Service Questions	Response	Definitions
Is this a service that was custom built for government? Do you Provide A Commodity Service	Yes	An information system service (e.g., telecommunications service) provided by a commercial service provider typically to a large and diverse set of consumers. The organization acquiring and/or receiving the commodity service possesses limited visibility into the management structure and operations of the provider, and while the organization may be able to negotiate service-level agreements, the organization is typically not in a position to require that the provider implement specific security controls.
CUI information is resident in the System (CUI data) (https://www.archives.gov/cui/registry/category-list)	Yes	If the service does not handle CUI, 800-171 may not be applicable A categorical designation that refers to unclassified information that does not meet the standards for National Security Classification under Executive Order 12958, as amended, but is (i) pertinent to the national interests of the United States or to the important interests of entities outside the federal government, and (ii) under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination.

GSA IT

NIST 171 v FedRAMP Qualifying Template - Section 3.b.1

Section 3.b.1- Essential Characteristics of Cloud Computing		Does the solution offering align to key characteristics of Cloud Service Offerings
On-demand self-service	No	Are solution resources by the user or by the provider to store handle or transmit Federal Data?
Broad network access	Yes	Is the system generally accessible over the internet over standard communication channels (web/api)
Resource pooling	Yes	The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and assigned according to consumer de… Are system resources and interfaces shared by multiple customers? …high… level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.
Rapid elasticity	Yes	Ca… Can the system rapidly expand to meet demands without prior coordination? …prov…oning often appear to be unlimited and can be appropriated in any quantity at any time
Measured service	No	Clou… Is the service billed/measured by a consumption model, such as software users, licenses or hardware resources? …act… transparency for both the provider and consumer of the utilized service.

GSA IT

NIST 171 v FedRAMP Qualifying Template - Section 3.b.2

Section 3.b.2 Utilizes a Cloud Deployment Model meeting conditions of 3.b.1		This section describes the deployment model used by components used to store Process or Transmit government CUI. I.
Private Cloud	No	Does the system use Private Cloud Services to handle CUI as part of its deployment
Community Cloud	No	Does the system use Community cloud services, I.E. a Gov specific cloud offering
Public Cloud	Yes	Does the system use Public commercial cloud service to handle CUI data?
Hybrid Cloud	No	Does the system use a mix of public, community and public cloud services?
N/A On-Premise not meeting 3.b.1 requirements	No	Is this system wholly hosted on premise on a system that does not meet the essential characteristics of cloud computing

GSA IT

NIST 171 v FedRAMP Qualifying Template - Section 3.b.2

Sec 3.c Cloud Service Models - Is the service offered as-a-service (e.g., Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS) as defined by NIST.		This inventories any cloud services used to store, process or transmit government CUI data.
IaaS	No	The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources [illegible] select networking components (e.g., host firewalls). Does the system provide IaaS services to the federal government for this use case? I.E. providing computing to run Federal Systems.
PaaS	No	The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired [illegible] configuration settings for the application-hosting environment. Does the system provide platform services to be used to collect or maintain data on behalf of the federal government.
SaaS	No	The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure [illegible] application capabilities, with the possible exception of limited user-specific application configuration settings. Does the system provide software services to be used to collect or maintain data on behalf of the federal government
N/A Cloud Hosted Shared Application not delivered "As a Service"	Yes	[illegible] the business service being provided. The system is a shared application that does not store or collect data for explicit federal usage, or on behalf of the federal government.

FedRAMP Requirements

- FedRAMP is a government-wide program that promotes the adoption of secure cloud services across the federal government by providing a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.
- Vendor solutions delivered as-a-service in the cloud, meeting NIST 800-145 cloud definition, consistent with the OMB FedRAMP Policy memo, are subject to FedRAMP cloud information security and privacy requirements.
- Vendors must be authorized at the FIPS 199 Moderate impact level.
- Third-Party Assessment Organization (3PAO) is required for assessment; recommended for documentation preparation. Vendor is responsible.
- FedRAMP Resources: https://www.fedramp.gov/

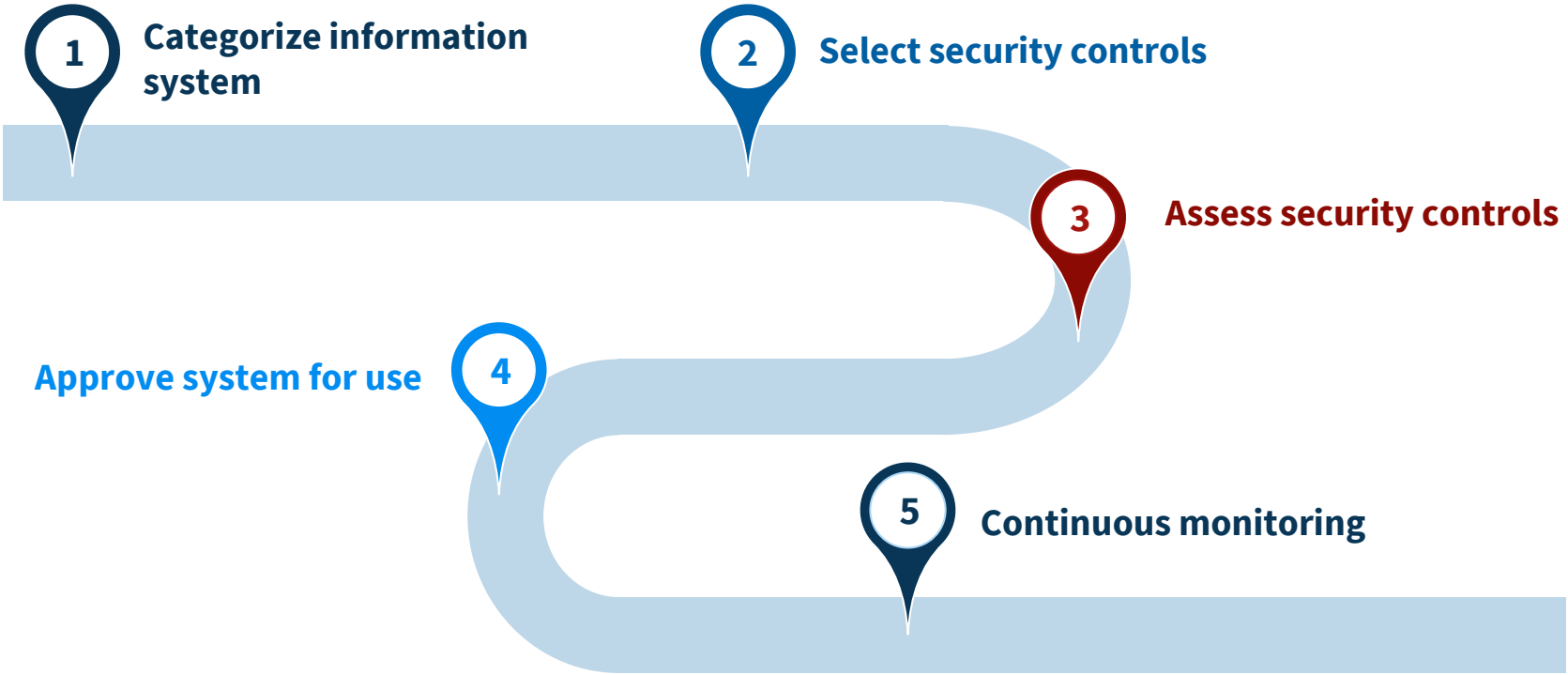
GSA Non-Federal Security & Privacy Review Process using NIST-171

Process Teams, Approval Process, General Process, Security Approval Package

GSA IT

Non-Federal Security Approval Process

Process derived from **Risk Management Framework (RMF)**



Process Team

GSA Program Functions

GSA Vendor Champion

- Coordinate Vendor & GSA IS groups
- Act as GSA Project Manager

CO/COTR

Contracting Officer/Contracting Officer Technical Representative

- Security acquisition language from GSA 09-48* is included in contract
- Compliance with security & privacy requirements on contract
- Timely delivery of deliverables (per contract and process)

GSA OCISO/Privacy Functions

GSA OCISO

Office of the Chief Information Security Officer

- Security of GSA info & systems
- Responsible for and approve use of NIST 171 review process for non-Federal vendor systems
- Security advisory & consultation ensuring compliance with GSA's Security Acquisition and NIST 800-171 Procedural guide

GSA Privacy Office

- Oversee GSA CUI Program
- Ensure compliance with GSA Privacy requirements
  - Review/approval of SORN, PTA, PIA & Privacy Controls

Vendor Partner Functions

Vendor 800-171 Team

- Agree to enter into 800-171 process
- Agree to C-SRM Monitoring
- Complete security package with GSA guidelines
- Contract with 3PAO to perform 800-171 assessment
- Submit quarterly & annual deliverables to GSA

3rd Party Assessment Org

- Assess system based on SSP
- Create Security Assessment Report

***Protecting Controlled Unclassified Information (CUI) in Nonfederal Systems and Organizations Process*

GSA IT

General Process Overview

Legend:
White Text: GSA Responsibility
Blue Text: Vendor/Assessor Responsibility

Kickoff and Package Preparation

Overview of GSA IS Nonfederal CUI Process

Provide Vendor GSA templates for vendor review

GSA Champion coordinates between Vendor and GSA IS

Security Control Selection

Vendor System Security Plan and package preparation

Package Review

GSA ISSO and ISSM SSP and PTA Review

GSA SecEng SSP Architecture review

GSA SSP Approval

GSA Security Assessment Plan (SAP) Approval

GSA Penetration Test Rules of Engagement (ROE) Approval *if deemed required

Documentation Update to Address GSA comments

Assess Sec and Priv Controls

3PAO assessment based on approved SSP, SAP and Test Cases

Vulnerability Scanning

Pentest (recommended)

Security Assessment Report (SAR) Report

PIA (if applicable)

Vendor Remediation of SAR findings

GSA Review and Approval

POA&M generated based on findings and recommendations of the SAR

Update System Security Plan based on SAR

GSA Review and approval to use

Continuous Monitoring

Quarterly deliverables
-Vulnerability Reports
-POA&M Updates

Annual deliverables
-System Security Plan
-PTA

3 Years
-System Security Plan
-Security Assessment
-PIA/PTA

GSA Review and Reissue approval to use

Vendor Update for GSA comments

GSA IT

Non-Federal Security Approval Package

- Package Deliverables
  - Signed System Security Plan
  - Privacy Threshold Analysis
  - Privacy Impact Analysis (if applicable)
  - Security Assessment Report
    - Signed Security Assessment Plan
    - OS vulnerability, OS configuration, and Web Application Vulnerability Scan Results
    - Assessment Test Cases
  - Plan of Action and Milestones
  - Penetration Test Results (Recommended)
  - C-SCRM Plan
  - SCRM Supplier Questionnaire

**GSA will provide templates for All documentation.

Questions?