IT Security Procedural Guide: Salesforce Platform Security Implementation CIO-IT Security-11-62

Revision 3

March 1, 2023

Office of the Chief Information Security Officer

VERSION HISTORY/CHANGE RECORD

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
		Version 1.x – September 12, 2019		
1	Jan Schober	Draft version 1.1 • Added User Permission File attachment • Updated Application Approval Process • Added Application Security Form and rearranged process steps	ISSM direction	P12 P7 P7
2	Jan Schober	Draft version 1.2 • Updated Application Approval Process, step 5. • Updated Application Security Assessment Form	ISSM direction	P7 P7
3	Jan Schober	Draft version 1.3 • Addressed PBS provided comments • Updated Application Approval Process PIA and Application Security Assessment Forms	ISSM direction	P1 P2 P6 P8

4	Jan Schober	Draft version 1.4
		• Updates made to section 2.2.1
		• Updates made to section 2.2.3, GSA NIST 800-53 Controls Spreadsheet file
		• Updates made to section 2.2.2 Application Approval Process file
		  ○ COE Process Flow
		  ○ Section 2, Step 5
		• Added Organization Baseline Security Configuration Settings file to section 2.2.4
			ISSM direction	P7
				P8

5	Jan Schober	Draft version 1.5 • Inserted Updated Baseline Security Configuration Settings Reference Guide file into section 2.2.4 • Inserted Security Controls Analysis file into Application Approval Process, Step 4.	ISSM direction	P8 P6
6	Blanche Heard	Draft version 1.5 • Accepted stakeholder comments/revisions.	OSAISO stakeholder review	Various
		Version 2.x – February 26, 2020		
1	Peter Nichols	Draft version 2.1 • Inserted Scanning Methodology in Section 9. • Corrected various grammatical/typographical errors. • Updated Application Review document. • Inserted Customer Access Methodology in Section 10. • Updated Section 8	ISSM direction	Various
2	Amy Reecer	Draft version 2.2 • Inserted updated timeout screenshot. • Inserted Customer Chatter Groups w/External Access in Section 11.	ISSM direction	P12 P15, P16

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
3	Peter Nichols	Draft version 2.3 • Update to Sub-System Application Approval Process Document • Update to Application Review Checklist	ISSM direction	
4	Blanche Heard	• IT Security POC/Stakeholder comments	OSAISO direction	Various
5	Peter Nichols	• Had a screen timeout setting of 30 min...when it should now be 60 • Changes made throughout the document to reflect NIST and GSA requirements	ISSM direction	Section 4.9 screen shot
6	John Sitcharing	• Included update of Rev 4 800-53 NIST controls and GSA requirements for procedural guide 06-30	Regular Update	Various
7	Dan Stanfield	Version 2.4 • Included updates related to SF App security	Regular Update	Various
8	Dean/Klemens	Version 2.5 • Updated style and formatting structure to align with current practices. • Renamed guide. • Updated Points of Contact	Regular Update	Various
		Revision 3 – March 1, 2023		
1	Adarkwa/Ricks/ Shepherd	• Updates included changes regarding: ○ AppExchange approval process ○ Approval changed from ATO to ATU ○ Updated links ○ Merged Organization and Application approval processes ○ Code scanning ○ External User Access ○ Approver from AO to ISSM	Periodic Update	Throughout
2	McCormick/ Klemens	• Edited, formatted to current style and guidance.	Periodic Update	Throughout

Approval

IT Security Procedural Guide: Salesforce Platform Security Implementation, CIO-IT Security 11-62, Revision 3, is hereby approved for distribution.

DocuSigned by:
Bo Berlas
FD717926161544F...

Bo Berlas
GSA Chief Information Security Officer

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

Table of Contents

Note: Hyperlinks in this guide may be restricted to internal GSA users (e.g., GSA Insite links) and, occasionally, to a subset of GSA users (restricted Google or Salesforce links).

1 Introduction

General Services Administration (GSA) has the capability to utilize commercial cloud computing services provided appropriate security controls are implemented, tested, and reviewed as part of the agency's information security program. These services are protected to the degree required by Federal Information Security Modernization Act (FISMA), FISMA implementing standards, and the most current GSA guidance. The Salesforce platform as a service (PaaS) and software as a service (SaaS) cloud computing offerings have unique attributes and require consistent risk management and continuous monitoring processes. Salesforce represents a new model for Information Technology (IT) development by offering extensive options for configuring workflows, databases, forms, dashboards and reports, process modeling, and customizable user interfaces. As a cloud solution, the Salesforce application configurations can take place without any requirements for hardware or software. In addition, the Salesforce platform, Force.com, offers two extremely valuable features by supporting mobile access and social business collaboration all from within the platform itself. Salesforce supports a standard method of application development therefore the potential for sharing and using the work of the entire GSA development community is immense.

Salesforce enables GSA to quickly and efficiently build applications to modernize our IT portfolio and promote innovative solutions in the areas of mobility, employee collaboration, shared development efforts and customer relationship management integration. Additional information on Salesforce can be viewed at the Salesforce Platform Security Center**.**

As described in CIO-IT Security-06-30: Managing Enterprise Cybersecurity Risk, GSA uses an Approval to Use (ATU) process for Salesforce organizations and applications. ATU is a risk-based approval process for usage of services, features, or functions on information systems or platforms with an existing Authorization to Operate (ATO).

2 Purpose

This guide assists GSA employees and contract personnel that have IT Security responsibilities, implement a standard Salesforce ATU process. The guide outlines the key activities for implementing the process.

3 Assumptions

- The procedures and policies outlined in this guide are incorporated into the IT Modernization Centers of Excellence (CoE) for GSA.
- Salesforce organizations are maintained by the Office of the Chief Information Officer (OCIO).
- Mandatory customer implemented organizational level settings identified in this guide are configured on all Salesforce organizations.
- Mandatory customer implemented application level settings identified are configured on all applications published on the Salesforce platform.

- Applications developed for internal GSA use are enabled with Multi-Factor Authentication (MFA) and will use Single Sign On (SSO). Access to these applications must be allowed from any location.
- Applications developed for external GSA use must have MFA enabled as deemed appropriate by the Business Owner and Information System Security Manager (ISSM).
- All applications developed will be reviewed and approved for IT security requirements as outlined in this guide. Coordination will occur between the Information System Security Officer (ISSO) and ISSM in this process.

4 GSA Salesforce Methodology

The following sections describe the overall Salesforce environment at GSA and the ATU process for Salesforce organizations and applications.

4.1 Salesforce Organization

Saleseforce.com, Inc. provides the Force.Com PaaS. The platform allows GSA developers to create and define unique "Org" instances in which individual applications are created.

These applications are built using Apex and Visualforce. AppExchange is a marketplace for cloud computing applications built for the Salesforce.com community and delivered by partners or by third-party purchased developer services, which users can purchase or download for free and add to their Salesforce.com environment.

AppExchange tool(s) must go through the GSA Chief Technology Officer (CTO) approval process for any new technology/software that has not been approved for use in the GSA environment. See the IT Standards Software Approval process for additional details.

4.2 GSA Salesforce Customers

The following GSA Salesforce Customer Organizations are designed to meet the unique business requirements described:

- **Enterprise Engagement Org (EEO)** - Focuses on GSA's role as an employer, supporting internal GSA collaboration and productivity.
- **Public Engagement Org (PEO)** - Focuses on GSA's role as a citizen resource by hosting the Federal Citizens Information Center, a citizen-facing call center for USA.gov and other government agency websites.
- **Government Engagement Org (GEO)** - Focuses on GSA's role as a government coordinator, supporting cross-government policy initiatives and data collection efforts.
- **PBS Client Solutions Org (CS)** - Focuses on GSA's role as a leasing organization, coordinating Public Buildings Service customer relationships and overseeing services to customers.
- **Property Disposal Org (PD)** - Focuses on GSA's role as a property manager, supporting the repositioning of unneeded government real property.

- **Workspaces Org (WS)** - Focuses on GSA's role as a property manager, providing workspace project management tools as well as a mechanism for allowing people and businesses to lease space to the government.
- **Customer Engagement Org (CEO)** - Focuses on GSA's role as a customer-facing sales organization by facilitating marketing, customer service, and sales activities for the Federal Acquisitions Service, as well as other GSA customer-centric forums and activities.

4.3 Salesforce Subsystem Customization

GSA Salesforce application customization will be done at the Organization level by adding customized applications to a Salesforce Organization. This includes adding sets of customized tabs for specific vertical- or function-level features (e.g., Finance, Human Resources, etc.).

4.4 Salesforce ATU Process

System Owners are responsible for ensuring that Salesforce Organizations and Applications have been through the GSA Salesforce ATU process and have received an ATU. The approval process for both Organizations and Applications is described in the subsections below.

4.5 Organization/Application Security ATU Process

A Salesforce Organization requires an ATU within GSA. Each new Salesforce Organization or application after completing the following process and upon acceptance/approval of the ATU package is integrated into an existing system's ATO package. The security approval process is the responsibility of the System ISSO working with the ISSM, Business Owner, System Development Team and the OCISO.

Step 1 – System Categorization – Complete a Federal Information Process Standard (FIPS)-199 Security Categorization template.

Step 2 – Complete a Privacy Threshold Assessment(PTA)/Privacy Impact Assessment (PIA) in GSA's implementation of Archer.

Step 3 – Application Assessment – First, determine whether other business processes are impacted should an outage or communication issue occur where the Salesforce platform is not available. If so, provide a mitigation/recovery strategy for the affected business process. This should be documented in the Salesforce App Review Template.

The Application Assessment also requires the development of an Application Configuration document, which records configuration details and characteristics of various components for the application. The results of this consideration of objects and configurations are summarized in the Application Review document.

Step 4 – Complete the following activities:

If an application was developed using Apex or Visualforce, code scans will be completed using scanning tools provided by Salesforce. Conduct static and dynamic scanning. The code scan results must be completed, and false positives must be adequately documented within the Application Review Form (provided in Step Five) prior to submitting the security package for approval. All critical/high findings must be remediated.

If the application was developed using an alternate language, coordination should take place with the OCISO early in the development process to coordinate code review methodology to be used.

Code scanning is done via Checkmarx. The report should be available for download from the Checkmarx site by the next business day.

A security self-assessment should be completed for Apex and Visualforce as described in the Salesforce App Review document completed as part of Step 5.

Step 5 – Complete the Salesforce App Review Template.

Step 6 - Prepare the Salesforce Application Security Package - Prepare the package (consisting of the items listed below) and submit it to the ISSM:

- FIPS-199 Security Categorization
- PTA/PIA
- Security Control Analysis
- Application Configuration Document
- Salesforce Application Review Document

Note: After the ISSM reviews and approves the package it becomes a part of the SSPP and allows the application to be added to the Salesforce inventory along with Plans of Action and Milestones (POA&Ms) reflecting any identified vulnerabilities.

4.6 NIST SP 800-53 Controls for Salesforce

Upon notification of a new application being developed for a Salesforce Organization or a new organization being established, the ISSO will request the current NIST SP 800-53 Controls for Salesforce Worksheet from FedRAMP. It provides the baseline security controls for a Salesforce Organization as well as the controls for an Application.

4.7 Salesforce Organization Baseline Security Configuration Settings

When a GSA customer uses a Salesforce Organization or Application, there are certain configuration responsibilities that must be implemented. The responsibilities are the customer security configurations that allow the cloud services to integrate properly and securely with GSA systems. The recommended security configuration settings to be applied to Salesforce

Organizations and Applications are provided in the Salesforce Organization Baseline Security Configuration Reference Guide (Example). It is the responsibility of the system ISSO to ensure periodic monitoring (weekly, monthly, or quarterly as per the direction of the ISSM) of the configuration settings at the Organization and Application level.

5 Salesforce Security Configuration Options Parameters

The Salesforce Security Configuration Options Parameters in the SF Security Settings document present the configurable user settings available to Organization Administrators. These parameters can also be used to further harden an Organization and subsequent Application for users. Some settings are included in the Salesforce Organization Baseline Security Configuration Reference Guide. Care should be used to analyze these controls before implementation to ensure that the customer-implemented controls are not affected. Any deviations to these settings must be documented in a Business Process Document (BPD) for the affected Organization.

6 Access Security

A key activity of application development and system configuration is access security. Security measures should not only protect data and logic from unauthorized external access, but also from unauthorized internal access. All users should be individually added to a role based on their need to know. The use of "View-All" and “Modify All” for groups should be minimized to the greatest extent possible.

7 Salesforce Profile Management Overview

Force.com provides a layered security framework that allows security administrators to create profiles, permission sets, roles, hierarchies, and rules that are enforced in the user interface. GSA uses Permission Sets to grant access to tabs and objects for a given application. To specify the fields a user can access, the administrator uses field-level security. To specify the individual records a user can view and edit, the administrator sets organization-wide defaults, defines a role hierarchy, and creates sharing rules. The Salesforce Guide to Sharing Architecture describes detailed concepts of the Salesforce security data access model. For further information about the access model and hands-on training, ISSO’s are encouraged to complete the following Salesforce security courses:

- Salesforce Data Security
- Salesforce Secure Identity and Access Management

7.1 Salesforce Navigation Tips

To access Salesforce Security configurations, select the "Setup" choice from the pull down menu below the userid name as shown in Figure 7-1.

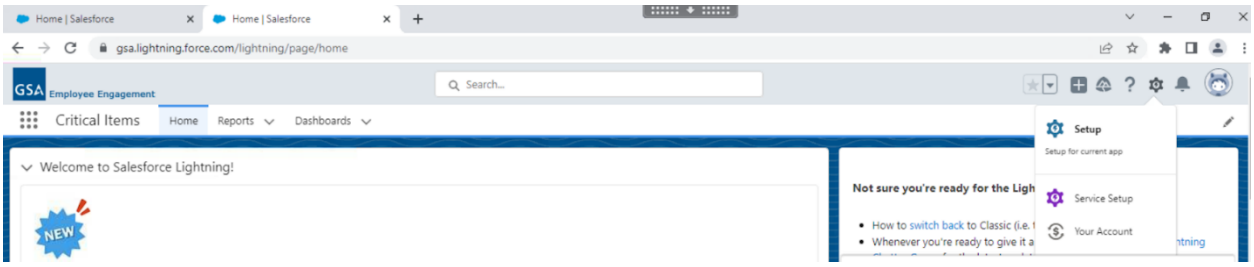

Figure 7-1. Setup Pull Down Menu

Figure 7-2 displays the Administration Setup configuration family which is available only to organization administrators.

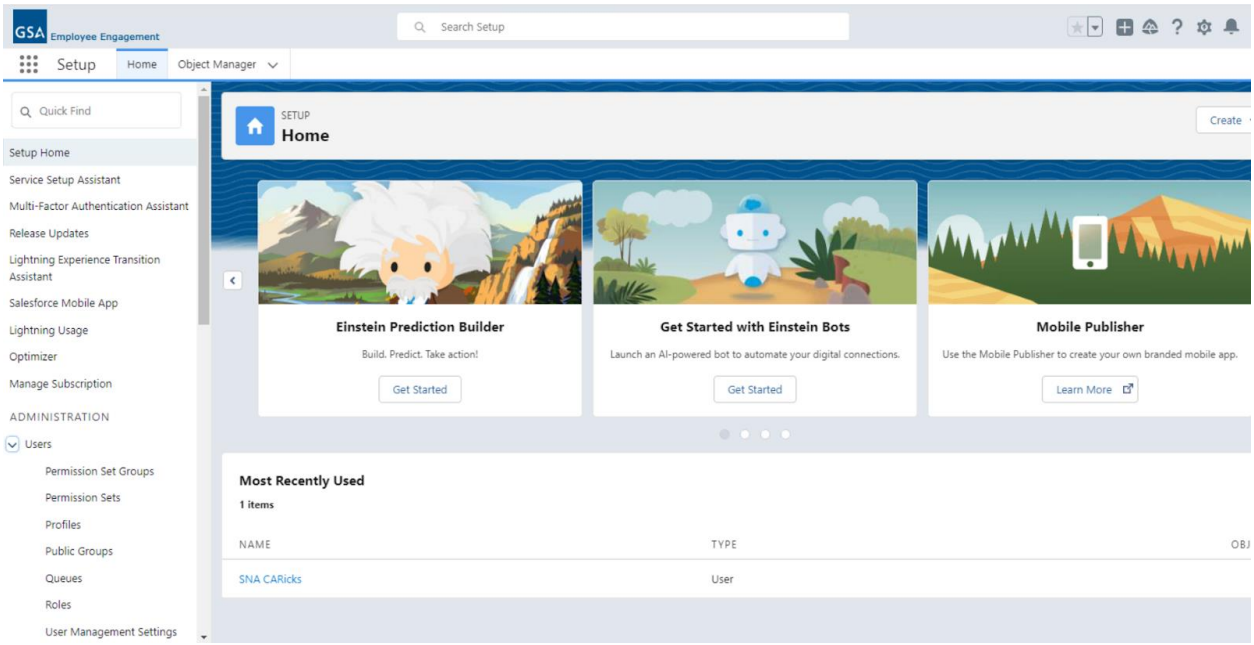

Figure 7-2. Administration Setup Configuration Family

The Administration Setup security configuration settings in Table 7-1 are named for the Individual Configuration area and the Sub-configuration area.

Table 7-1. Salesforce Administration Setup Security Relevant Sub-Groups

Configuration Area	Sub-Groups	Page Blocks
Manage Users	• Roles • Profiles	
Security Controls	• Sharing Settings • Field Accessibility • Password Policies • Session Settings • Network Access • Package Support Access • Certificate and Key Management • Single Sign--On Settings • Identity Provider • View Setup Audit Trail • Expire All Passwords • Delegated Administration • Remote Site Settings • HTML Documents and Attachments Setting • Portal Health Check	
Mobile Administration	Salesforce Mobile	– Configurations – Users and Devices – Settings
	Chatter Mobile	– Settings – Users and Devices
	Mobile Dashboards	
Desktop Configuration	• Outlook Configuration • Offline Briefcase Configurations • Chatter Desktop Settings	
Email Administration	• Deliverability • Organization-Wide Addresses • Compliance BCC Email • Test Deliverability • Email to Salesforce • Delete Attachments Sent as Links • Email Footers	
Google Apps	Settings	

The actual settings are implemented by changing the field settings of the Subgroup page to the GSA required value. Fields vary and can take the form of check boxes, radio buttons, pull-down menus, or open text. Figure 7-3 depicts the Sessions Settings sub-group page.

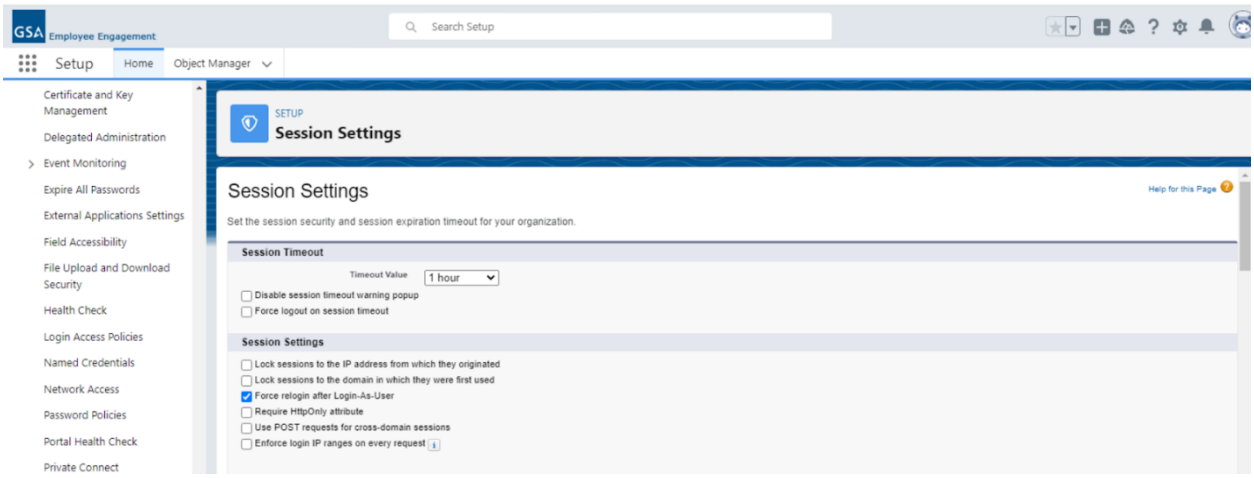

Figure 7-3. Session Settings Sub-group Page

8 Salesforce User Permissions

An up to date listing of Salesforce out of the box Profiles can be found at Salesforce Standard Profiles. The standard profiles may need to be modified by GSA teams.

9 External Customer Access

Government employees and contractors who are not credentialed within the GSA infrastructure, but have PIV compliant access within their own agency, may have a business need to have limited access to the GSA's Salesforce resources. There are several ways to accomplish this, depending on the level of risk to the information:

- **Salesforce Communities and Portals**: The Salesforce CRM customer community is true self-service software as a service (SaaS); designed so that external customers can help themselves to similar tools as internal users. The external users must use GSA approved MFA authentication via customer portals.
- **Customer Chatter Groups**: This method provides outside entities with access to Salesforce Chatter. This method is more targeted around a project or program, and not for general outreach. The group owner will be manager of the Chatter group and is responsible for implementing the policy that no documents will be posted in their respective group and must use SF access control. See Section 11 for further details.
- **External Access Accounts**: The account holder must comply with Homeland Security Presidential Directive 12 (HSPD-12) and GSA's IT Security Policy.

9.1 Salesforce Customer Community Authentication

Applications with external user access requirements for moderate data will be accessed via Salesforce Communities secured to MFA using Login Flows or Office of Management and Budget (OMB) MAX authentication. Organization owners are responsible for provisioning of the Communities and coordinating setup and support with the Salesforce CoE (for MFA). MFA is required for ALL users/administrators.

9.2 Procedure to Acquire External Access Accounts

Any external user accessing GSA information systems that contain moderate impact data must be adjudicated fully under the HSPD-12 guidelines for their agency prior to being granted access to GSA systems. At a minimum this must be a Tier 1 adjudication. If the requestor holds a National Security clearance or a Public Trust investigation higher than a Tier 1, the type and date of the adjudication must be indicated. This information is verified by the requesting Agency Security Officer and indicated by signatory authority from that Agency (which may be the assigned System ISSO, ISSM or HR personnel, according to that Agency's policy) on the External Access to Salesforce Users form attached to the request.

9.3 Processing External Access Accounts

The steps for provisioning External User Access are as follows:

Step 1 – A ServiceNow ticket must be opened to provision an External user (EXT domain).

Step 2 – After the ticket is created, verify it has a 'Name' and 'Non-GSA' Email address in it.

Step 3 – Assign the ticket FIRST to the Directory Services assignment group called GSA.CO-ENT-Directory Services in order to get the EXT User ID account created.

Step 4 – Upon completion, Directory Services should re-assign this ticket to the GSA.OCIOAppSupport queue, along with the EXT User ID account for the user.

Step 5 – Search for the user's Federation ID using the Name and Email Address in the Directory Service information.

Step 6 – If user Federation ID is found continue to step 9.

Step 7 – If user Federation ID is not found, immediately notify the Directory Services department by forwarding the ticket back to Assignment Group: GSA.CO-ENT-Directory Services.

Step 8 – The Directory Services team will return the ticket once they have generated a Federation ID for the user.

Step 9 – At this point, we have Federation ID, Name, Email and EXT User ID associated with the user.

Step 10 – Update the task with the external user name (User ID) and Federation ID (Email address should already have been supplied during initial request).

Step 11 – Now, create a Contact record for the user and associate it with an appropriate account.

Step 12 – Convert the contact to a portal account (Add Federation ID).

Step 13 – Retrieve the external user name (EXT User ID) from the Directory Services information and send it to the App Owner/ticket requester.

Step 14 – Enter Level of Effort (LoE) in the Worknotes section and mark the task as Completed.

10 Scanning of the Salesforce Environments

The Force.com Security Source Code Scanner service is available on the Partner Security Portal and provides custodians and developers of the Force.com platform information regarding the security of their code (specifically Apex and Visualforce) through next generation static analysis tools. The Salesforce code scanner service runs Checkmarx, a commercial scanning tool. GSA also hosts an internal Checkmarx tool for scanning Force.com. Due to reliability issues with the free Salesforce scanning service, all code scans of GSA Orgs are run using GSA's internal tool. Scans are run using the "GSA_Baseline_PortalAll-rev3" preset.

A code scan is performed only on the entire organization/sandbox, so that any error will be reflected upon any application within that organization/sandbox. The following process dictates the LoE for the use of the vulnerability scanning service by organization:

Development Sandboxes: When an app is first built, developers do their code reviews by scanning the code themselves.

Quality Assurance (QA) Sandboxes: The QA team scans the app as part of their QA process to ensure it was coded properly before it gets pushed to user acceptance testing (UAT).

User Acceptance Testing Sandboxes: The System ISSO or System Operations and Maintenance (O&M) team runs the scan on behalf of the UAT process. That scan should be run once any expected changes have been completed. This sandbox is also the PreProd/Staging/Integ sandbox.

Production: All Salesforce System ISSOs shall provide a monthly scan report of their production Salesforce Environment Org to the OCISO via the email address saiso-salesforce-scan-reports@gsa.gov. Any Medium, High, or Critical vulnerabilities shall be noted explicitly in the email; include the business justification from the Application Review. Any High or Critical issues must be remediated within 30 days of discovery and Medium issues within 60 days of discovery.

11 Customer Chatter Groups with External Access

Private Groups in Chatter allow users to segregate conversations, files, and posts from the main GSA Chatter population. They allow teams, groups, and partners to work together on projects and issues without worry that others might become privy to the information they share or post. Customer Chatter groups in GSA also allow for a feature not seen before in the Agency, that being, the ability of GSA users to collaborate in real time with non-GSA employees. Examples of these people are other agency employees, vendors, customers, and others GSA does business with on a daily basis. With Customer Chatter groups, a group owner can invite non-GSA personnel to work as a collaborative team in private and have their work kept away from public Chatter feeds in Salesforce. Chatter group owners have the responsibility to ensure their group is maintained, monitored and the data shared among members is not sensitive or otherwise critical to GSA's operations.

GSA users that wish to create a Customer Chatter Group that allows outside customer access must read and acknowledge the Rules of Behavior (RoB) for GSA's Customer Chatter Groups with Outside Users. To complete and submit a Rules of Behavior (ROB) agreement, go to Private Chatter Groups (this link is restricted, contact app-support@gsa.gov if access is needed). Additionally, all members of a Customer Chatter Group must comply with GSA Order CIO 2104.1, "GSA's IT Rules of Behavior." Private group owners are accountable for the actions of all group members and should ensure any member invited is made aware of the Customer Chatter Group and GSA IT Rules of Behavior.

Private group owners are responsible for maintaining a list of all group members and their email addresses for audit purposes. As such, group owners are responsible for daily auditing of the posts and files within their group, ensuring any unacceptable posts are immediately removed. An OCISO audit will be performed monthly by the system ISSO of randomly selected groups to capture a representative sample of the authorized groups.

The following actions will be performed when groups are found to be non-compliant with the RoBs agreed to by group owners will:

- The system ISSO will notify the group to immediately remove the non-compliant content.
- The system ISSO will verify the non-compliant content has been removed.
- If the non-compliancy discovered as part of the audit review generates an investigation due to the nature of the content, the investigation will be coordinated within GSA's incident response capability by creating an initial and follow up report and submitting it to the OCISO IR Team.

Any group found non-compliant is subject to immediate deletion without prior notification.