LEVERAGING SALESFORCE U.S. GOVERNMENT AUTHORIZATIONS

Overview

Federal, state, and local government organizations, along with government contractors trust Salesforce to deliver critical business applications, in large part because of Salesforce's commitment to security and privacy. This white paper provides an overview on how these organizations can leverage the Salesforce Government Cloud's Federal Risk and Authorization Management Program (FedRAMP) Moderate and Department of Defense (DoD) Information Impact Level 4 (IL4) authorizations and the Salesforce Government Cloud Plus' FedRAMP High authorization to approve usage of Salesforce within U.S. Government organizations. U.S. Federal organizations can evaluate these offerings and approve their specific implementation using the Risk Management Framework (RMF) as documented in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems, and Department of Defense Instruction (DoDI) 8510.01, RMF for DoD Information Technology, and determine how to maintain compliance with U.S. Government or industry-specific requirements.

FedRAMP Authorizations

To assist organizations that are required to comply with U.S. public sector requirements while delivering critical business applications, Salesforce's information security programs for the Salesforce Government Cloud and Government Cloud Plus are aligned with the FedRAMP requirements at the Moderate and High impact levels, respectively. FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. The FedRAMP approach uses a "do once, use many times" framework with the goals of accelerating the adoption of secure cloud solutions through reuse of assessments and authorizations, and achieving consistent security authorizations using a baseline set of agreed-upon standards to be used for cloud product approval. FedRAMP is the result of close collaboration with cyber security and cloud experts from the General Services Administration (GSA), NIST, Department of Homeland Security (DHS), DoD, National Security Agency (NSA), Office of Management and Budget (OMB), the Federal Chief Information Officer (CIO) Council and its working groups, as well as private industry.

The Salesforce Government Cloud achieved its initial Authority to Operate (ATO) at the Moderate impact level granted by the U.S. Department of Health and Human Services (HHS) in May 2014. The Salesforce Government Cloud Plus achieved its Provisional ATO (P-ATO) at the High impact level granted by the FedRAMP Joint Authorization Board (JAB) in May 2020.

Customers should ensure data within their Salesforce Customer Orgs do not exceed the authorized impact level of the Salesforce environment they are using. For example, privacy

information (including Personally Identifiable Information (PII)) should fall into the moderate range in accordance with NIST SP 800-60 Revision 1 Volume 1, Guide for Mapping Types of Information and Information Systems to Security Categories, meaning both the Salesforce Government Cloud and Government Cloud Plus are appropriate.

DoD Authorizations

The DoD Cloud Computing Security Requirements Guide (CC SRG) requirements, designed by the Defense Information Systems Agency (DISA), leverages the FedRAMP assessment process and adds additional security controls and requirements necessary to meet the DoD's critical mission requirements. A Cloud Service Provider (CSP) Cloud Service Offering (CSO) is assessed in accordance with the criteria outlined in the DoD CC SRG, with the results used as the basis for awarding a DoD Provisional Authorization (PA) at the applicable information impact level. Once the DoD PA is granted, the CSP is expected to maintain the security posture of the CSO through continuous monitoring as required by FedRAMP and also include additional information for DoD requirements.

Both the Salesforce Government Cloud and Government Cloud Plus have received DoD authorization for IL2 via reciprocity based on their FedRAMP authorizations. At this level, DoD Mission Owners may use these environments for publicly releasable data, along with low-sensitivity PII and unclassified information categorized up to low confidentiality and moderate integrity (L-M-x). The Salesforce Government Cloud has also received DoD authorization for IL4, which is appropriate for Controlled Unclassified Information (CUI), including PII and Protected Health Information (PHI), or other mission-critical data to include that used in direct support of military or contingency operations categorized up to moderate confidentiality and moderate integrity (M-M-x).

Authorization Boundaries

Both the Salesforce Government Cloud and Government Cloud Plus are dedicated instances of Salesforce's industry-leading Platform as a Service (PaaS) and Software as a Service (SaaS), multi-tenant community cloud infrastructure specifically for use by U.S. federal, state, and local government customers, U.S. government contractors, and Federally Funded Research and Development Centers (FFRDCs).

The Salesforce Government Cloud and Government Cloud Plus authorization boundaries are composed of the backend infrastructure that support operations, referred to as the General Support System (GSS), and the following Salesforce services: Lightning Platform, Sales, Service, Communities, Einstein Analytics, and Industry Solutions.[1] Applications available on the Salesforce AppExchange are not included in the authorization boundary

[1] For more information, see https://help.salesforce.com/articleView?id=000321821.

defined by Salesforce. If an organization wishes to implement an application available in the AppExchange, they should evaluate the application on an individual basis in accordance with their assessment and evaluation processes prior to its deployment. More guidance on this topic is available in this Salesforce Knowledge Article.

To maintain compliance with FedRAMP and DoD requirements for services included in the Salesforce Government Cloud and Government Cloud Plus authorization boundaries, Salesforce conducts security assessments and authorization activities using NIST SP 800-53, Security and Privacy Controls in Federal and Information Systems and Organizations, the moderate baseline control set consistent with the requirements set forth in the Federal Information Security Modernization Act (FISMA) of 2014,[2] NIST SP 800-37, and FedRAMP, HHS,[3] and DoD guidance.

Salesforce also conducts continuous monitoring of its security controls that includes ongoing technical vulnerability detection and remediation, remediation of open compliance-related findings, and an annual independent security assessment. Annual security assessments of the Salesforce Government Cloud and Government Cloud Plus are conducted by a FedRAMP approved third-party assessment organization (3PAO) using test plans in accordance with NIST SP 800-53A, Assessing Security and Privacy Controls in Federal and Information Systems and Organizations, as well as FedRAMP and DoD requirements. The security assessment testing determines the adequacy of the security controls used to protect the confidentiality, integrity, and availability of the Salesforce Government Cloud and Government Cloud Plus and the customer data it stores, transmits, and processes.

Leveraging Salesforce U.S. Government Authorizations

Once a CSO achieves a FedRAMP or DoD authorization, organizations can leverage the authorization package to address their own compliance needs. To approve their usage of the Salesforce Government Cloud or Government Cloud Plus, each organization should review Salesforce's authorization materials and make a risk-based decision on acceptance of the controls provided by Salesforce. The security controls provided by Salesforce allow organizations to focus on the policies and technical configurations for usage of their specific Salesforce Org.

The primary benefit of a FedRAMP or DoD authorization is that agencies can reuse the existing security assessment and authorization package for the cloud solution to leverage work already performed by the CSP, 3PAO, and, when applicable, the Authorizing Agency. Process efficiencies, cost reduction, and increased speed to cloud adoption can be realized during the risk acceptance and approval process when organizations deploy their own

[2] For more information, see https://www.dhs.gov/fisma.
[3] HHS is the agency sponsor for the Salesforce Government Cloud FedRAMP Moderate ATO.

business applications on Salesforce. While the FedRAMP website and DoD CC SRG describe the high level process to leverage a FedRAMP or DoD authorization, organizations can utilize the process described in subsequent sections of this white paper to specifically deploy and authorize Salesforce Government Cloud and Government Cloud Plus services for their use.[4]

Available Documentation

The Salesforce Government Cloud and Government Cloud Plus FedRAMP/DoD authorization packages materials include the following:

FedRAMP/DoD Package Materials	
System Security Plan (SSP)	The System Security Plan documents Salesforce's implementation of the relevant FedRAMP and DoD security controls. Controls include an implementation status and control origination. The implementation status specifies the operational status (i.e., Implemented, Partially Implemented, Planned, Alternative Implementation, Not Applicable) of the control. Controls identified as Planned have an associated POA&M item. The control origination identifies the party responsible for implementing the control. Control origination can include Salesforce (Service Provider Corporate, Service Provider System Specific, Service Provider Hybrid), the customer (Configured by the Customer, Provided by the Customer), or both Salesforce and the customer (Shared). Controls where the customer has some responsibility to implement include a Customer Responsibilities section in the control implementation description. The Customer Responsibilities section specifies the specific action/responsibility the customer must perform to implement the control.
Partner SSP	Summarizes control implementation status information from SSP for implementation partners, state and local government customers, and government contractors.
Customer Configuration User Guide	Recommends technical settings that customers should configure in their Salesforce organization to meet various customer or industry-specific requirements.
E-authentication Worksheet	Describes the processes for establishing user identities electronically presented to the Government Cloud or Government Cloud Plus as defined in OMB Memorandum M-04-04.
Privacy Impact Assessment (PIA)	Analysis of the environment to determine if any components collect PII, and if so the type of PII collected, and the functions that collect it.
Rules of Behavior	Describes the security controls associated with user responsibilities and specific expectations of behavior for following security policies, standards, and procedures.

[4] Organizations should ensure compliance with all executive orders, mandates, governance, and organization-specific requirements with regards to the authorization and onboarding of new services that store, process, or transmit federal information.

Contingency Plan	Supports contingency planning and disaster recovery requirements for FedRAMP and DoD by denoting interim measures to recover services following an unprecedented emergency or system disruption.
Configuration Management Plan	Describes the hardening, configuration management, and ongoing configuration management processes, which are considered as the basis for establishing secure configuration settings required for infrastructure supporting the environment.
Incident Response Plan	Provides incident response roles, responsibilities, processes, and definitions.
Control Implementation Summary (CIS) Workbook/Customer Responsibilities Matrix (CRM)	Delineates the control responsibilities between Salesforce and customers. In addition, the CIS Workbook provides a summary of all required FedRAMP and DoD controls and enhancements across the environment. The CRM reviews controls that customers are responsible for implementing to comply with FedRAMP and DoD control requirements.
Inventory Workbook	Consolidates all of the inventory information (hardware, network, and software) required to support annual continuous monitoring reporting.
Continuous Monitoring Materials	
Continuous Monitoring Plan	Details the frequency that applicable security controls are reviewed and assessed by Salesforce.
Plan of Action and Milestones (POA&M)	Documents detailed information on open technical vulnerabilities and control gaps within the environment based on periodic scanning and external audit assessments, including planned remediation actions and remediation timeframes. As the POA&M is also a "living document," agencies should ensure they are reviewing the current version of the POA&M to have an accurate understanding of open weaknesses and the plans for remediation. The POA&M is updated monthly as part of standard continuous monitoring activities.
3PAO Audit Reports	
Security Assessment Plan (SAP)	Details a 3PAO's plan for security assessment testing. Once completed, this document constitutes a plan for testing security controls during the annual audit.
Security Assessment Report (SAR)	Provides a framework for the 3PAO's evaluation of the implementation of and compliance with security controls and the applicable results. The SAR describes the testing approach, includes findings from the testing, and documents a risk rating for each of the findings at the time of testing.
Security Requirements Traceability Matrix (SRTM)	Documents the assessment testing and results performed by the 3PAO during annual audits.
SAR Findings Table	Describes security control failures identified by the 3PAO during the annual audit.

Obtaining Documentation

As trust is Salesforce's number one value, we protect our customer's data by ensuring the processes that support the Salesforce Government Cloud and Government Cloud Plus align with this goal. Salesforce's FedRAMP and DoD authorization packages include detailed information about Salesforce's infrastructure and security program that protects our customer's data. Therefore, we treat the FedRAMP and DoD authorization packages as Salesforce Proprietary and Confidential and limit secure distribution of the documentation to eligible organizations. Additional security measures implemented on the documentation ensure the confidentiality and integrity of the contents are protected. Organizations provided the documentation may not copy/paste and should not reproduce data from the documentation into any of their documentation or implementation materials since Salesforce materials can be referenced in their entirety.

To obtain Salesforce's FedRAMP or DoD authorization package materials, please follow these steps:

U.S. Federal Government Organizations

1. **Request Documentation:** Download the Package Access Request Form available on the FedRAMP Marketplace[5] at either https://marketplace.fedramp.gov/#/product/salesforce-government-cloud (Salesforce Government Cloud) or https://marketplace.fedramp.gov/#!/product/salesforce-government-cloud-plus (Salesforce Government Cloud Plus).
    - Information that should be used for the Package Access Request Form includes:
        - Email Address: Requestor's .gov or .mil email address.
        - Name of Package Requested: Either "Salesforce Government Cloud" or "Salesforce Government Cloud Plus". To obtain DoD-specific content, append "DoD" to the offering name.
        - Package ID: "AGENCYSF" for the Salesforce Government Cloud or "FR2003061248" for the Salesforce Government Cloud Plus.
    - Once completed, submit the form to info@fedramp.gov.
2. **Access Documentation:**
    - For the Salesforce Government Cloud, access will be granted to the documentation hosted on OMB MAX (https://portal.max.gov/).
        - FedRAMP materials are available at https://community.max.gov/x/eQs3Kw.

[5] Process described at https://www.fedramp.gov/accessing-csps-fedramp-materials-omb-max/.

- DoD materials are available at https://community.max.gov/display/FedRAMPExternal/Salesforce+-+DoD.
- To find latest POA&M: Salesforce Continuous Monitoring -> Salesforce POA&M & Inventory.
- To find latest SSP and SSP Attachments: Salesforce Continuous Monitoring -> Salesforce Annual Assessments -> Salesforce AA 20XX.
- Additional Note: The Salesforce Initial ATO Assessment folder is NOT the latest version of our documentation. This is from our initial assessment in 2014 and should only be used for historical purposes.

o For the Salesforce Government Cloud Plus, access will be granted to a secure portal hosted by Salesforce. You will be notified promptly by Salesforce once access is granted.

Other Eligible Organizations (Government Contractors, FFRDCs, Implementation Partners, and State/Local Governments)

1. Contact your Salesforce Account Executive and request available Salesforce Government Cloud or Government Cloud Plus FedRAMP or DoD authorization materials.[6]
2. Complete the standard Salesforce Non-Disclosure Agreement (NDA) if not already a customer or under NDA.
3. For the Salesforce Government Cloud:
    a. Complete the Salesforce Government Cloud Compliance Information NDA.
    b. A link to Salesforce Government Cloud documentation will be provided via email.
4. For the Salesforce Government Cloud Plus, access will be granted to a secure Salesforce-hosted portal where you will be presented with a click-through Salesforce Government Cloud Compliance Information NDA. Access to documentation will subsequently be granted.

Applying Documentation to the RMF

Customers looking to leverage Salesforce Government Cloud or Government Cloud Plus FedRAMP and DoD authorizations should reference Salesforce's FedRAMP and DoD

[6] Authorization package materials available for Non-U.S. Federal Government Customers include the Partner SSP, CIS/CRM, and Customer Configuration User Guide.

authorization package materials and document the specific controls that their organization implements for their instance of Salesforce, which supplement the security controls inherited from Salesforce as outlined in the FedRAMP and DoD authorization packages. To assist with their review, customers can follow the six steps outlined in the RMF Process:

1. Determining Security Categorization
2. Selecting Security Controls
3. Implementing Security Controls
4. Assessing Security Controls
5. Authorizing Use of the Information System
6. Monitoring Security Controls

Determining Security Categorization

Salesforce customers should conduct security categorization as an organization-wide activity taking into consideration applicable requirements and how they plan to use Salesforce. This will allow the customer to categorize their usage of Salesforce and the level of data that will be stored and processed based on the mission and business objectives of their organization. The customer should consider results from their organization risk assessments as a part of their security categorization decision to be consistent with their risk management strategy to identify potential impact to mission/business functions resulting from the loss of confidentiality, integrity, and/or availability. Security categorization determinations should also consider potential adverse impacts to the customer's organization. The determined security categorization should influence the selection of appropriate security controls for the customer's use of the Salesforce Government Cloud or Government Cloud Plus, and also, where applicable, minimum assurance requirements.

For more information on how the Salesforce Government Cloud or Government Cloud Plus security categorization was determined, please see the SSP - Attachment 10 FIPS 199 Categorization.

Selecting Security Controls

Once the security categorization of the information system is determined, the Salesforce customer should select applicable security controls accordingly. This can be done by selecting an applicable security control baseline (e.g., FedRAMP Moderate, DoD IL4) and be tailored accordingly to align the controls with the specific conditions within their organization to address conditions related to organizational risk tolerance, mission/business functions, other information systems, or customer operational environments.

While Salesforce has implemented security controls at the FedRAMP Moderate and DoD IL4 levels for the Government Cloud and at the FedRAMP High level for the Government Cloud Plus, please contact your Salesforce Account Executive to discuss other compliance frameworks or privacy regulations which are not covered in the Salesforce FedRAMP and DoD authorization packages.

For more information on how the Salesforce Government Cloud or Government Cloud Plus address security controls within the identified control baselines, please see:

- SSP
- CIS
- PIA

Implementing Security Controls

Salesforce customers should use best practices when implementing the security controls within their organization to align with applicable requirements and their usage of Salesforce. In addition, customers should ensure that mandatory processes and configuration settings are established and implemented in accordance with their policies and industry standards, while understanding what controls they will inherit from Salesforce. To determine what security controls are inherited from Salesforce and what is the responsibility of the customer to implement, organizations should refer to Salesforce Government Cloud and Government Cloud Plus authorization package materials, specifically for controls designated as having a "Customer Responsibility."

When implementing security controls, organizations should document how they meet applicable requirements. This documentation formalizes plans and expectations regarding the overall functionality of their use of the Salesforce Government Cloud or Government Cloud Plus while providing a description of security control's functionality and how they were implemented to comply with requirements.

For more information on what security controls the customer inherits from the Salesforce Government Cloud or Government Cloud Plus and what the customer is responsible for, please see:

- SSP
- CIS/CRM
- Customer Configuration User Guide

Assessing Security Controls

Once the organization has implemented security controls, they should also develop, review, and approve a plan to assess these controls. The organization should test their

implementation of security controls to address applicable requirements, especially those designated as having "Customer Responsibilities" in the Salesforce Government Cloud or Government Cloud Plus FedRAMP and DoD authorization packages for their specific implementation of Salesforce.

The organization should also review 3PAO reports to assess how security controls they inherit from Salesforce are addressed. These reports should be leveraged and referenced during their assessment of security controls to gain a full understanding of how the organization is able to meet applicable requirements.

For more information on what security controls the customer can inherit from the Salesforce Government Cloud or Government Cloud Plus and what the customer is responsible for, please see the following authorization package materials:

- SSP
- E-Authentication Worksheet
- PIA
- Rules of Behavior
- Contingency Plan
- Configuration Management Plan
- Incident Response Plan
- CIS/CRM
- 3PAO Reports:
    - SAP
    - SAR
    - SRTM
    - SAR Findings Table

Authorizing Use of the Information System

Once a customer has reviewed the security authorization package, has implemented and assessed the security controls for their specific implementation of Salesforce, and fully understands the residual risks of the solution, the organization should:

- Make a risk-based decision on whether they will accept the security controls implemented from Salesforce.
- Make a risk-based decision on whether they will accept the security controls implemented for their specific implementation of Salesforce.
- Approve the organization's implementation of Salesforce Government Cloud or Government Cloud Plus.

Monitoring Security Controls

To maintain compliance with applicable requirements as well as ensure the operational effectiveness of security controls, Salesforce customers should implement a continuous monitoring program that can identify deficiencies and vulnerabilities to their use of the Salesforce Government Cloud or Government Cloud Plus, and document these findings with recommendations for actions that can be taken to resolve these issues.

For more information regarding the status of Salesforce continuous monitoring activities for the Salesforce Government Cloud or Government Cloud Plus, please see:

- Continuous Monitoring Plan
- POA&M[7]

Document Disclaimer

Although Salesforce has attempted to provide accurate information and guidance in this document, Salesforce provides no warranty or assurances related to its content. The implementations, procedures, and policies of Salesforce are subject to change and may impact the information reflected in this document. The rights and responsibilities of the parties with regard to your use of Salesforce's online software services shall be set forth solely in the applicable agreement executed by Salesforce. Customers, including those who purchase services on the Salesforce Government Cloud, should make their purchase decisions based upon features that are currently available. This document is subject to Salesforce's Forward-Looking Statements at: https://investor.salesforce.com/about-us/investor/forward-looking-statements/.

[7] Organizations who have specific questions about a POA&M should contact their Salesforce Account Executive.