Salesforce Government Cloud

Security White Paper

November 2018

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 of Salesforce's principles of trust and compliance specifically for the Salesforce Government Cloud in the context of the Federal Risk and Authorization Management Program (FedRAMP) and the Department of Defense (DoD) Cloud Computing Security Requirements Guide (CC SRG). Subsequent sections introduce the security and privacy features inherent to the Salesforce Government Cloud that customers can use to build and secure their applications and customer data. The security and privacy features that help achieve compliance with required controls, derived from National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," are referenced in brackets throughout this document.

Salesforce Government Cloud

To support the security and compliance needs of our U.S. public sector customers, Salesforce launched the Salesforce Government Cloud. The Salesforce Government Cloud is a dedicated instance 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 isolated production infrastructure supporting the Salesforce Government Cloud customer data ensures that the physical hardware in Salesforce's colocation data centers that process, store, and transmit Government customer data are separate from hardware supporting other customers. While isolated, the underlying infrastructure supporting the Salesforce Government Cloud is the same trusted architecture model that supports Salesforce's multi-tenant public cloud offering and over five billion customer transactions a day.

The Salesforce Government Cloud information system and authorization boundary is comprised of the following Salesforce services[1]:

- Lightning Platform
- Sales
- Service
- Communities
- Einstein Analytics

Features of these services include:

- Content
- Ideas
- Knowledge
- Chatter messenger, Chatter files, and customer-facing Chatter groups
- Salesforce Shield[2]: Platform Encryption, Event Monitoring, and Field Audit Trail
- Salesforce Industry Applications: Health Cloud and Financial Services Cloud

---

[1] A list of current in-scope Salesforce products included in the authorization boundary is available at: https://help.salesforce.com/articleView?id=Government-Cloud-available-products-and-features&language=en_US&type=1

[2] For additional information on Salesforce Shield, please see: https://www.salesforce.com/products/platform/products/shield/.

The backend infrastructure (servers, network devices, databases, storage arrays), referred to as the General Support System (GSS), support the operations of the Salesforce products.

For more information on Salesforce Government Solutions please see:
https://www.salesforce.com/solutions/industries/government/overview/

Principles of Trust

Salesforce's vision is to be the government's trusted cloud PaaS and SaaS provider, based on the values of maintaining confidentiality, integrity, and availability of customer data. Salesforce's methods to fulfill this vision are built upon an executive commitment to maintain and continuously improve the security of the Salesforce Government Cloud and include:

- **Defense-in-depth** – Whenever possible, multiple controls and technologies are applied to limit the possibility of any single point of failure
- **Investment** – To manage, analyze, and improve security effectiveness, invest in personnel, tools, and technologies
- **Transparency** – Trust cannot be maintained without open communications regarding service performance and reliability. Salesforce strives to be industry leaders in transparency. Trust.salesforce.com is the Salesforce community's home for real-time information on system performance and security. On this site you'll find:
    - Up-to-the minute information on planned maintenance
    - Phishing, malicious software, and social engineering threats
    - Best security practices for your organization
    - Information on how we safeguard your data

Salesforce Compliance Maturity

As a leading PaaS and SaaS provider, data security and compliance are paramount for Salesforce. Salesforce serves over 150,000 customers and processes over five billion transactions a day. The organizations that use Salesforce include customers in heavily regulated industries such as financial services, healthcare, insurance, and public sector that require strict adherence to security and privacy requirements. To meet the compliance needs of these customers, Salesforce continually raises the bar of security.

Salesforce has undergone SSAE 16 SOC 1 (previously known as SAS 70 Type II) examinations semi-annually since 2004. Salesforce also completes SOC 2 and SOC 3 for Service Organizations audits and has achieved compliance with PCI-DSS. In May 2008, Salesforce became the first publicly traded SaaS vendor to receive the prestigious ISO/IEC 27001 Security Certification (ISO 27001) company-wide and service-wide, addressing applicable controls including our data centers and major offices worldwide. As the only internationally accepted security standard, ISO 27001 ensures security best practices and a managed approach to business information protection, and helps Salesforce provide a consistent, reliable and secure operating environment to its customers worldwide. In May 2014, Salesforce achieved a FedRAMP Agency Authority to Operate (ATO) at the moderate impact level issued by the Department of Health and Human Services (HHS) for the Salesforce Government Cloud[3]. Based on this ATO, the

[3] See the FedRAMP Marketplace at: https://marketplace.fedramp.gov/#/product/salesforce-government-cloud

Defense Information Systems Agency (DISA) granted a DoD Impact Level 2 (IL2) Provisional Authorization (PA) to the Salesforce Government Cloud and, subsequently in 2017, granted an IL4 PA to the Salesforce Government Cloud[4].

Federal Risk and Authorization Management Program (FedRAMP)

Salesforce's information security program for the Salesforce Government Cloud is aligned with the FedRAMP requirements at the moderate impact level.

To obtain compliance with FedRAMP, Salesforce conducted security assessment and authorization activities in accordance with FedRAMP guidance, NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Lifecycle Approach, and HHS guidance. In accordance with NIST SP 800-18, Guide for Developing Federal Information System Security Plans, Salesforce documented a System Security Plan (SSP) for the Salesforce Government Cloud service offering. The SSP identifies control implementations for the GSS and in-scope customer-facing products (Lightning Platform, Sales, Service, Communities, Einstein Analytics, and Industry Solutions) according to the FedRAMP Moderate baseline and HHS security control parameters. In accordance with NIST 800-53A and FedRAMP Moderate requirements, a third-party assessment organization (3PAO) conducted a security assessment of the Salesforce Government Cloud. The security assessment testing determined the adequacy of the management, operational, and technical security controls used to protect the confidentiality, integrity, and availability of the Salesforce Government Cloud and the customer data it stores, transmits, and processes.

To maintain compliance with FedRAMP, Salesforce conducts continuous monitoring, which includes ongoing technical vulnerability detection and remediation, remediation of open compliance related findings, and at least annual independent assessment of a selection of security controls.

Department of Defense (DoD)

In addition to a FedRAMP Moderate ATO, the Salesforce Government Cloud has received Provisional Authorizations (PA) from DISA at IL2 and IL4, based on DISA's Cloud Computing Security Requirements Guide (CC SRG). This allows DoD Mission Owners to use the Salesforce Government Cloud to manage non-mission critical Controlled Unclassified Information (CUI), including PII and Protected Health Information (PHI).

The Salesforce Government Cloud has also received a Cloud Approval to Connect (CATC) from DISA, which allows DoD Mission Owners to connect Salesforce to a DoD Cloud Access Point (CAP) after they are granted a Cloud Permission to Connect (CPTC).

Information Security Governance

Information security governance is a term that encompasses all the tools, people, and business processes an organization uses to ensure the security and privacy of the data that its systems maintain. Salesforce's approach to information security governance is structured around the ISO 27001/27002 framework and consistent with the requirements identified in NIST SP 800-53, and includes many components:

---

[4] See the DoD Cloud Computing Catalog at: https://www.disa.mil/-/media/Files/DISA/Services/Cloud-Broker/DoD-Cloud-Service-Catalog.ashx

- **Employees** – Employees receive regular information security training. Employees in data-handling positions receive additional role-based training specific to their roles *[AT-2, AT-3].*
- **Security Staff** – Salesforce has dedicated security staff supporting the system *[PM-2].*
- **Counsel** – Salesforce has a team of Privacy Counsel, Compliance, and Government Contracts Attorneys who are responsible for ensuring compliance with global privacy laws, international regulatory regimes, and federal procurement regulations.
- **Assessments** – Salesforce regularly conducts both internal vulnerability assessments (for example, architecture reviews by security professionals, vulnerability scans) as well as external third-party audits and external vulnerability assessments (for example, vulnerability assessments by managed security services providers, or MSSPs) *[RA-5, SI-2].*
- **Policies and Procedures** – Detailed internal policies dictate how Salesforce handles various aspects of the security and compliance governance. Examples of security policies and procedures include: Incident Response Plan, Datacenter Access Procedures, Configuration Management Plan, etc. *[IR-1, PE-1, CM-1]*

In particular, Salesforce incorporates security into its development processes at all stages. From initial architecture considerations to post-release, all aspects of software development incorporate security. The following describes some of the standard practices Salesforce employs, which help make it the trusted provider that it is today.

- **Design phase** – Guiding security principles and security training help ensure Salesforce engineers make the best security decisions possible. Threat assessments on high-risk features help to identify potential security issues as early in the development lifecycle *[SA-3, SA-8].*
- **Development phase –** Salesforce addresses standard vulnerability types through the use of secure coding patterns and anti-patterns, and uses static code analysis tools to identify security flaws *[SA-10].* Secure code development during design, development, and release is controlled through a secure code repository.
- **Testing phase –** Internal Salesforce staff and independent security consultants use scanners and proprietary tools along with manual security testing to identify potential security issues *[SA-11].*
- **Prior to release** – Salesforce validates that the functionality being developed and maintained meets its internal security requirements. Code is tested and approved prior to release. Post-release, Salesforce uses independent security service providers to analyze and monitor the product for potential security issues. Reports on these findings are made available to prospects and customers under a non-disclosure agreement *[SA-11].*

Shared Security and Compliance Model

With Salesforce PaaS and SaaS, data security and compliance are a shared responsibility with customers. While Salesforce provides secure and compliant services to protect customer data and applications, customers are ultimately responsible for properly configuring and operating those services as required by their organization.

As depicted in the figure that follows, with legacy on-premise systems, organizations have sole responsibility for maintaining the security and compliance of the entire IT stack. This can drain resources and prevent ongoing IT modernization. It can also introduce risk and impact compliance. While Infrastructure as a Service (IaaS) may alleviate some burden, organizations still need to upgrade and patch software, worry about dependencies within the stack, and independently implement many security controls.

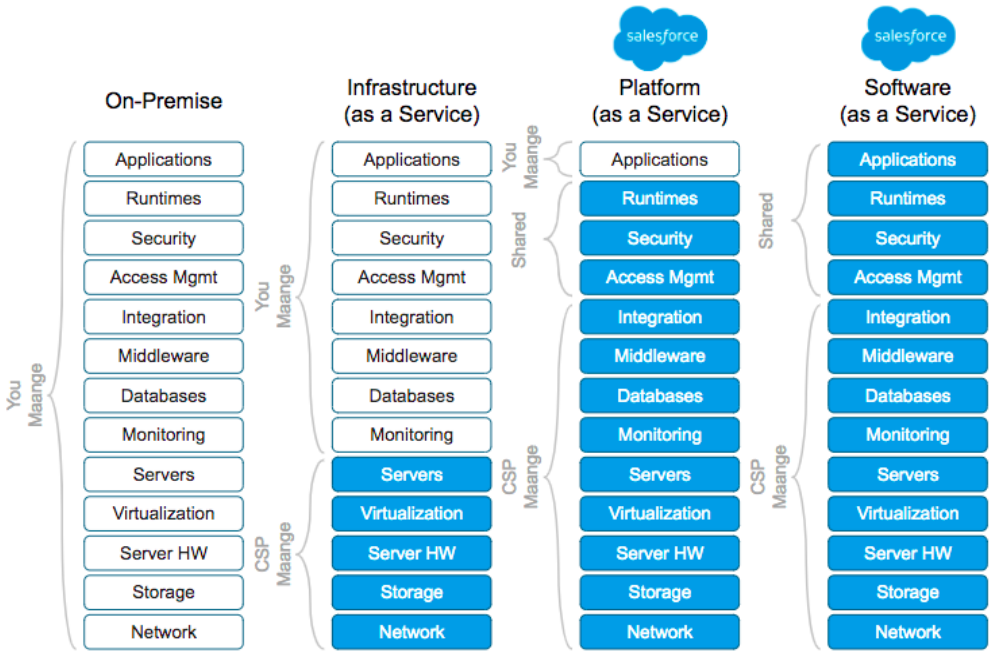

Figure: Delivery Models

With Salesforce, customers inherit the majority of security controls from Salesforce. While customers do bear some responsibility for ensuring security and compliance, Salesforce provides numerous enablement resources, including training and implementation guides. Specifically, for customers seeking compliance with FedRAMP Moderate or DoD IL2 / IL4, Salesforce provides a Customer Configuration Guide tailored to those requirements. This shared responsibility model greatly reduces both risk and burden for customers, allowing them to place more focus on their business and mission.

Platform Security

The figure at the right illustrates the many layers of defense the Salesforce Government Cloud uses to resist various types of threats and achieve compliance with security frameworks such as DoD IL4, DoD IL2, FedRAMP, SSAE 16 SOC 1, SOC 2, SOC 3, ISO 27001, and PCI-DSS–all without sacrificing application performance.

At the infrastructure layer, Salesforce strictly manages access to its facilities and the work engineers can perform once inside a facility [PE-2]. Before being granted access, employees must pass a thorough Salesforce background check [PS-3]. After a person is authorized for logical access, they can access the production network using secure methods, such as private networks, stringent segregation of duties, and least privilege [AC-2, AC-5, AC-6, IA-2].

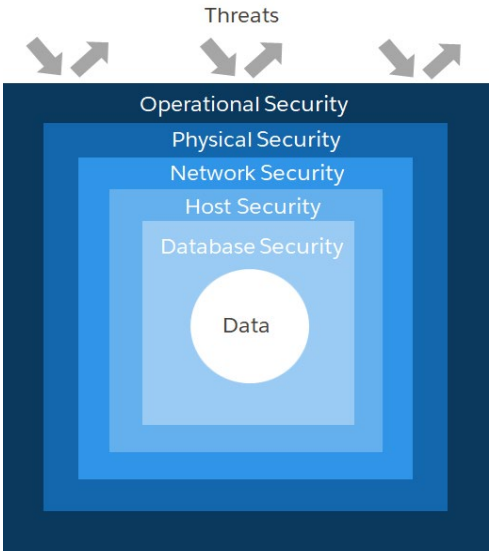

Figure: Salesforce incorporates security at multiple layers to protect against threats

Qualified Personnel

For the Salesforce Government Cloud, additional controls have been implemented around personnel management. Access to systems inside of the Salesforce Government Cloud storing U.S. government, U.S. government contractors, and FFRDC customer data that potentially permit access to customer data are restricted to Qualified U.S. Citizens. Qualified U.S. Citizens are individuals who are United States citizens, are physically located within the United States when accessing the Salesforce Government Cloud systems, and have completed a background check as a condition of their employment with Salesforce. Research and development personnel and personnel that provide Administration Services under Government Cloud Premier + Success Plan support, who have logical access to customer data, and infrastructure support personnel that provide Government Cloud Premier + Success Plan support who have physical access to the Salesforce Government Cloud infrastructure, are Qualified U.S. Citizens.

Multi-tenancy

The Salesforce service is delivered using a multi-tenant model. The multi-tenant architecture and secure logical controls address separation of customer data.

The Salesforce infrastructure is divided into a modular architecture based on "instances." Each instance is capable of supporting multiple customers in a secure and efficient manner. Salesforce uses the instance architecture to scale and meet the demands of our customers. There are appropriate controls in place designed to prevent any given customer's implementation of Salesforce from being compromised. This functionality has been designed and undergoes robust testing through an ongoing process by both Salesforce and its customers [AC-2, SC-4].

Physical and Environmental Controls

Customer data in the Salesforce Government Cloud is processed and stored in two U.S. colocation data centers within dedicated secure spaces. Salesforce's hardware is located inside secure server rooms designated to Salesforce and separated by concrete walls from other data center tenants. Individual racks inside of the data center's Salesforce server rooms are further secured with locked cabinets that only authorized Salesforce personnel can open. Specific racks are allocated for hardware supporting the Salesforce Government Cloud. Access to the racks supporting the Salesforce Government Cloud hardware is restricted to Qualified U.S. Citizens as described in the prior section, Qualified Personnel.

Data centers provide only power, environmental controls, and physical security. Salesforce employees manage all other aspects of the service at the data centers. Colocation data center personnel do not have network or logon access to the Salesforce systems. Colocation personnel have physical access to the Salesforce secure server room in the event of an emergency, but do not have keys to the individual racks containing hardware.

The exterior perimeter of each anonymous data center building is bullet resistant, has concrete vehicle barriers, closed-circuit television coverage, alarm systems, and manned 24/7 guard stations that together help defend against non-entrance attack points. Inside each building, multiple biometric scans and guards limit access through interior doors and to the Salesforce secure rooms at all times.

Access to Salesforce's secure server rooms in the datacenter is authorized based on position or role. Additional access controls enforced by an electronic key box are implemented for the dedicated Salesforce Government Cloud racks to ensure that access is limited to Qualified U.S. Citizens. Salesforce

has an established process to review data center access logs to the server room. Additionally, an assessment of the data center is performed at least annually to ensure the data centers are meeting Salesforce's security control requirements *[PE-2, PE-3]*.

In addition to securing the data center locations, it is imperative that the data center facilities maintain robust critical infrastructure to support Salesforce through the following services:

Temperature and Humidity Controls *[PE-14]*

- Humidity and temperature control
- Redundant (N+1) cooling system

Power *[PE-11]*

- Underground utility power feed
- Redundant (N+1) CPS/UPS systems
- Redundant power distribution units (PDUs)
- Redundant (N+1) diesel generators with on-site diesel fuel storage

Secure Network Logistics *[CP-8, PE-4]*

- Concrete vaults for fiber entry
- Redundant internal networks
- Network neutral; connects to all major carriers and located near major Internet hubs
- High bandwidth capacity

Fire Detection and Suppression *[PE-13]*

- VESDA (very early smoke detection apparatus)
- Dual-alarmed, dual-interlock, multi-zone, pre-action dry pipe water-based fire suppression

Network Protection

Salesforce secures its network on many different fronts; for example:

- **End-to-end TLS** cryptographic protocols encrypt network data transmissions between the customer to Salesforce *[SC-8(1)]*.
- **Network gateways and firewalls** at the external network boundary are configured by default to deny all traffic and allow by exception, filtering unwanted network traffic. If necessary, they apply traffic rate limits. Filter events are logged and monitored for anomalies. *[CM-7, SC-7, SC-7(3)]*.
- **Stateful packet inspections** (SPI) firewalls inspect all network packets and prevent unauthorized connections *[SC-7]*.
- **Intrusion detection sensors** are placed throughout the network monitor traffic and report events to a security logging and alerting system for logging, alerts, and reports *[AC-4, SC-7, SI-4]*.
- **Secure routing and traffic flow policies** ensure that customer traffic is encrypted entering Salesforce until the load balancer decrypts the traffic. The load balancers decrypting the traffic are FIPS 140-2 compliant and are located inside of the Salesforce Government Cloud isolation boundary. Network devices enforce traffic flow policies in the Salesforce Government Cloud *[SC-4, SC-5, SC-7, SC-7(3), SC-7(4), SC-8, SC-8(1)]*.
- **Denial-of-Service (DoS) protection** is provided using a multi-layered approach utilizing high

availability, traffic monitoring, anomaly detection, and a third-party DoS mitigation service. Salesforce uses multiple Internet Service Providers (ISPs) to ensure redundancy of connections and increased availability. Monitoring is performed continuously and we have a contract with a third-party DoS mitigation service, should an active DoS attack be discovered *[SC-5].*

Logical Access Controls

Salesforce has implemented strong logical access controls for the production network, including:

- **Authorized users** are granted production access after manager approval and based on business justification. Terminated users are removed in a timely manner *[AC-2].*
- **Two-factor authentication processes** verify the authentication of access requests to internal systems *[IA-2(1), IA-2(2)].*
- **Bastion Hosts** act as hardened barriers between the authentication perimeter and core servers *[AC-2, IA-2, IA-2(1)].*
- **Segregation of duties and least privilege** is enforced to ensure that employees are granted only the necessary level of access to the production network to perform their assigned job functions based on role *[AC-5, AC-6].*
- **Infrastructure logging** is enabled to capture system activity and logs are forwarded to a central logging system *[AU-2].*

Configuration and Change Management

Salesforce implements industry-accepted best practices to harden underlying systems that support the various software layers of the service [*CM-2, CM-6*]. For instance, hosts are configured with non-default software configurations and minimal processes, user accounts, and network protocols. Hosts log their activity in a remote, central location for safekeeping. Salesforce has performed a review of device configurations against industry best practices and required standards for government markets [i.e., the Center for Internet Security (CIS) Benchmarks] (where available) to ensure devices are configured securely [*CM-6, CM-6(1)*].

Change Management processes dictate that system changes and maintenance are documented in Salesforce's internal ticketing system. Changes require approval, testing, and security impact analysis prior to deployment [*CM-3, CM-4*]. In addition, any changes that constitute a significant change, per Salesforce's significant change definition, require analysis and an impact assessment to determine impact to the Salesforce Government Cloud Authority to Operate [*CA-6*].

Database Security

The underlying database layer plays a significant role in platform security. For example, the database protects customer passwords by storing them via the SHA algorithm with a 256-bit one-way hash.

Salesforce enforces strict control of database administrator access to only authorized individuals with a business justification for access [*AC-2, IA-2(8), IA-5, IA-5(1), IA-5(6), IA-5(7)*]. Databases are configured in accordance with security benchmarks provided by industry best practices and required standards for government markets (i.e., the CIS Benchmarks) [*CM-6*]. Databases undergo periodic vulnerability assessments to check the databases for known vulnerabilities [*RA-5*].

Operational Monitoring

The Salesforce application and website are monitored on a 24x7 basis for reliability and performance.

- The Site Reliability (SR) team monitors the service and has subject matter experts (SMEs) in various disciplines. The SR handles first-and second-tier support, with technical engineers providing escalation support.
- Overall system monitoring is provided by a variety of tools and alerts are aggregated.
- Monitoring tools are automated and route issues, warnings, and problems to the Site Reliability teams.
- Alerts of events of significance are routed to the on-call personnel as well as to the engineering teams.

Salesforce has built extensive monitoring and instrumentation into the application itself so that the application can accurately report its health and performance to on-call support staff and engineers [*IR-2, MA-3, PM-6*].

Security Monitoring

A variety of tools, third-party resources, and a dedicated Computer Security Incident Response Team (CSIRT) provide comprehensive monitoring of the Salesforce production environment. These include:

- **Intrusion Detection Systems (IDS)** – IDS monitor the production network for potentially malicious network traffic *[AC-4, SC-7, SI-4].*
- **Logging and Alerting System** – Activity logs from production devices and servers are sent to a logging and alerting system that reports and alerts on events *[AC-2(4), AU-2, AU-6, SI-4].*
- **Threat Monitoring** – The Salesforce security team receives and reviews threat alerts from a variety of sources including SANS, United States Computer Emergency Readiness Team (US-CERT), and Open Web Application Security Project (OWASP). Threats that are deemed critical are escalated to the appropriate resource to respond *[SI-5].*
- **Vulnerability Scanning** – Vulnerability scans are performed on a periodic basis to check hosts for known vulnerabilities. Vulnerabilities are remediated in accordance with established remediation timeframes *[RA-5].*
- **Perimeter monitoring** – Third-party security firms provide periodic vulnerability scanning and continuous perimeter monitoring to detect vulnerabilities and alerts on security related incidents *[RA-5, SI-2].*
- **Security Incident Monitoring** – The CSIRT monitors for security incidents. Identified security incidents are handled in accordance with the Incident Response Plan *[IR-4].*

Incident Response

Salesforce maintains an Incident Response Plan and has an established Security Incident Response process. Salesforce will notify customers in the event Salesforce becomes aware of an actual or reasonably suspected unauthorized disclosure of customer data. Notification may be made by any of the following methods: phone contact by Salesforce support, email to customer's administrator and Security Contact (if submitted by customer), and/or public posting on trust.salesforce.com. [*IR-4, IR-6, IR-8*].

Government customers can report security incidents related to their Salesforce products and offerings via security_gov@salesforce.com. Salesforce will respond in accordance with the incident response process.

Disaster Recovery and Backup

The Salesforce service performs replication at each data center. Annual disaster recovery tests for the service verify the projected recovery times, as well as the data replication between the production data center and the disaster recovery center. The disaster recovery site is a warm site intended to contain equal capacity of the primary production site (host, network, storage, data). Data is transmitted between the primary and disaster recovery data centers across encrypted links. Additionally, back-ups of data are performed and data is retained on backups at the geographically separated disaster recovery data center location [*CP-4, CP-6, CP-7, CP-9, MP-5*].

Media Protection and Sanitization

Salesforce has an established process for protecting and sanitizing media as required by FedRAMP and DoD IL2 / IL4. Salesforce controls and securely stores backup disks and hard drives within data center facility secure areas until sanitized or destroyed using the physical security controls previously mentioned [MP-4]. Salesforce media containing customer data is not physically transported outside of these controlled areas without first being sanitized using a seven pass wipe or destroyed [MP-6].

Platform and Application Security

The Salesforce Government Cloud provides extensive features and tools that provide security for the data generated by customers. Customers can use many of these features to implement security policies governing exactly who, what, from where, when, and how users can access specific IT applications and data, and meet related auditing requirements.

The default user authentication mechanism for the Salesforce Government Cloud requests that a user provide a username and password (credentials) to establish a connection. The Salesforce Government Cloud does not use cookies to store confidential user and session information [*AC-2, IA-2*].

Many organizations use single sign-on mechanisms to simplify and standardize user authentication across a portfolio of applications [*IA-2(1), IA-2(2), IA-5, IA-5(1)*]. The Salesforce Government Cloud supports two single sign-on (SSO) options:

- **Federated authentication** using Security Assertion Markup Language (SAML) allows a session to send authentication and authorization data between affiliated but unrelated Web services.
- **Delegated authentication** enables an organization to integrate cloud applications with an authentication method of choice, such as a Lightweight Directory Access Protocol (LDAP) service or authentication using a token instead of a password.

Customers can implement multi-factor authentication by integrating with one of Salesforce's SSO capabilities [*IA-2(1), IA-2(2)*]. Specifically, customers who require user authentication via Government-issued smart cards, such as a Common Access Card (CAC) or Personal Identity Verification (PIV) card, can implement federated authentication to authenticate users via a SAML assertion generated by their identity provider (IdP).

The Salesforce Government Cloud offers several features to further confirm the identity of a connection request. For example, when a user requests a connection for the first time using a new computer-browser-IP address combination, Salesforce notices this request, sends an email to the user, and requests that the user confirm his/her identity by clicking the activation link in the email [*IA- 2(1)*].

User authentication and identity confirmation determine who can log in, and network-based security features limit the time and location from where users can log in. When an organization imposes IP address restrictions and a connection request originates from an unknown address, the connection is denied, helping protect data from unauthorized access and "phishing" attacks [*SC-7(3), SC-7(4)*].

To protect established sessions, the Salesforce Government Cloud monitors and terminates idle sessions after a configurable period of time. Session security limits help defend system access when a user leaves his/her computer unattended without first disconnecting [*AC- 11*].

Login profiles provide organizations an efficient way to manage system and application access for sets of similar users. First, an administrator creates a profile that controls access to entire applications, specific application tabs (pages), administrative and general user permissions, and object permissions [CRUD (create, read, update, delete)], along with other settings. Then, the administrator assigns each user a login profile. If the common requirements for a set of users change, the administrator simply updates the login profile for that group of users, instead of applying updates to every individual user [*AC-2, AC-5, AC-6*].

The Salesforce Government Cloud provides a flexible, layered sharing design that lets an organization expose specific application components and data sets to different sets of users *[AC-2, AC-5, AC-6, SC-2]*:

- **User profiles** – An organization can control the access its users have to objects by customizing profiles. Within objects, organizations can then control the access users have to fields using field-level security. Sharing settings allow for further data access control at the record level.
- **Sharing settings** – Organization-wide default sharing settings provide a baseline level of access for each object and let the organization extend that level of access using hierarchies or sharing rules. For example, an organization can set the default access for an object to Private when users should only be able to view and edit the records they own, and then create sharing rules to extend access of the object to particular users or groups.
- **Sharing rules** – Sharing rules allow for exceptions to organization-wide default settings that give additional users access to records they don't own. Sharing rules can be based on the record owner or on field values in the record.
- **Manual sharing** – When individual users have specific access requirements, owners can manually share records. Although manual sharing is not automatic like organization-wide defaults, role hierarchies, or sharing rules, it lets record owners share particular records with particular users, as necessary.

By request, the Salesforce Government Cloud can also require users to pass a user verification test (CAPTCHA) to export data. This simple text-entry test helps prevent malicious automated programs from accessing an organization's data.

The Salesforce Government Cloud has a multitude of history tracking and auditing features that provide valuable information about the use of an organization's applications and data, which in turn can be a critical tool in diagnosing potential or real security issues [*AU-2, AU-6, AU-7, AU-11*]. Auditing features include:

- **Record Modification Fields** – All objects include fields to store the name of the user who created the record and who last modified the record. This provides some basic auditing information.

- **Field History Tracking** – Customers can also enable auditing for individual fields, which will automatically track any changes in the values of selected fields and retain the data for 18 months. Although auditing is available for all custom objects, only some standard objects allow field-level auditing.
- **Field Audit Trail (additional subscription option)** – With Field Audit Trail, customers can retain field history data for up to 18 months and define object-level policies to retain archived field history data up to 10 years from the time the data was archived. This feature helps customers comply with industry regulations related to audit capability and data retention.
- **Login History** – Customers can review a list of successful and failed login attempts to your organization for the past six months within Salesforce by accessing Login History.
- **Identity Verification History** – With Identity Verification History, administrators can review their org users' identity verification attempts, such as when using a time-based one-time password for two-factor authentication, for the past six months.
- **Setup Audit Trail** – Administrators can view a Setup Audit Trail for the past six months within Salesforce, which logs when modifications are made to an organization's configuration. While the Login History, Identity Verification History, and Setup Audit Trail are available for six months within Salesforce, these audit trails can be downloaded or exported via API and stored locally to meet longer audit log retention requirements *[AU-11]*.
- **Event Monitoring (additional subscription option)** – Event monitoring provides granular level logging data, which monitors user activity within Salesforce. Event log can be retrieved via API or analyzed within the Event Monitoring Analytics App. Administrators can view information about individual events or track trends in events to identify abnormal behavior and safeguard data *[AU-2, AU-6, AU-7].* Customers seeking compliance with DoD IL4 requirements must implement Event Monitoring.

Finally, Salesforce administrators can identify and fix potential security risks and vulnerabilities with their Salesforce org from a single page using Security Health Check. This feature assesses security settings against an established baseline and calculates a summary score. Salesforce provides a baseline standard, while administrators can upload up to five custom baselines. Additionally, for the Salesforce Government Cloud, Salesforce provides a baseline tailored to FedRAMP Moderate and DoD IL2 / IL4 requirements. For more information, please see: https://help.salesforce.com/articleView?id=security_health_check.htm&type=5

Logical Security

The Salesforce Government Cloud's innovative metadata-driven, multi-tenant database architecture delivers operational and cost efficiencies for cloud-based applications without compromising the security of each organization's data.

- When a user establishes a connection, the user is assigned a client hash value associated with the session.
- During login, the authenticated user is mapped to their org and access privileges according to the sharing model *[AC-5, AC-6].*
- Along with the formation and execution of each application request, the application confirms that the user context [an organization ID (orgID)] accompanies each request. It includes it in the WHERE clause of all SQL statements to ensure the request targets the correct organization's data. The application validates that every row in the return set of a database query matches the session's orgID *[SC-4]*.
- Before the rendering of a web page that corresponds to an application request, the application

confirms that the calculated client hash value matches the client hash value that was set during the login phase *[SC-4]*.
- An error in the query process does not return any data to the client *[SI-11]*.

Data Ownership

Salesforce will maintain customer access to customer data; however, customer data is owned by the customer. Customers can use Export Services utilities to extract their data, including: weekly export (for applicable products), data loader, APIs, EAI tools, etc.

Data Retention

Active customer data stays on disk until the customer deletes or changes it. Customer-deleted data is temporarily available (15 days) to customers online from the recycle bin. Backups are rotated every 90 days (30 days for sandboxes); therefore, changed or deleted data older than 90 days (30 days for sandboxes) is unrecoverable.

Salesforce customers are responsible for complying with their company's data retention requirements in their use of the Salesforce services. If a Salesforce customer must preserve data and the retention procedures above are insufficient, they may export their data at no charge as part of the applications' applicable Export Services utilities previously discussed, or may create a sandbox account for storage of this data. Exports of customer data are otherwise available in comma separated value (.csv) format by request via Salesforce's Customer Support department for a fee. In addition, an org administrator can manually pull many exports detailing system usage and other data.

Protecting PII

Salesforce has conducted a Privacy Impact Assessment (PIA) for the delivery of the Salesforce service. The Salesforce service is rated as a moderate impact system. As such, Salesforce has implemented security controls aligned with the FedRAMP Moderate and DoD IL4 security baselines and are assessed against both by an independent third party assessor at least annually [*PL-5*].

Customers are responsible for conducting their own PIA for customer data stored in Salesforce. NIST SP 800-60 provides guidance to organizations on categorizing an information system, and states that for personally identifiable information (PII), the confidentiality impact level should generally fall into the moderate range. Salesforce recommends that federal agencies relying on our FedRAMP ATO and DoD IL2 / IL4 PAs determine the Security Categorization of their data to ensure the data stored in Salesforce does not exceed the moderate impact level [*PL-5*].

As outlined in the previous sections, the Salesforce Government Cloud has numerous configurable security features that allow customers to customize security based on the sensitivity of the data customers store in the application, consistent with the requirements in NIST SP 800-53 for moderate impact systems. One such security feature is encryption. The Salesforce service provides the ability to encrypt fields and files. Customers can implement Classic Encryption for selected custom fields, or, with Platform Encryption (additional subscription option), customers can encrypt a variety of widely used standard fields, many custom fields and files and attachments. Encrypted fields utilize AES-128-bit keys for Classic Encryption and AES-256-bit keys for Platform Encryption. Platform Encryption also allows customers to manage the encryption key lifecycle. The encryption libraries for both Classic Encryption and Platform Encryption are FIPS 140-2 validated [SC-13, SC-13(1)]. Additional security controls are

detailed in Salesforce's Security Implementation Guide:
http://resources.docs.salesforce.com/sfdc/pdf/salesforce_security_impl_guide.pdf.

Privacy

At Salesforce, there is no higher priority than the privacy and security of our customers' data. We believe that protecting the privacy of our customers' data is integral to our mission of earning and maintaining the trust of each of our customers. We seek to lead the industry as a trusted repository for customer data through a world-class privacy program and provide a secure infrastructure and flexible tools that help enable our customers to comply with global privacy and data protection regulations.

Privacy Statement: https://www.salesforce.com/company/privacy/

For detail on privacy protection at Salesforce:
http://content.trust.salesforce.com/trust/en/learn/protection/

For information on the Global Privacy Law Landscape: http://www.trust.salesforce.com/trust/learn/laws

Other Customer Considerations

State and Local Governments

Many state and local government customers require the implementation of NIST SP 800-53 controls for a commercial Cloud Service Offering (CSO), while others now require a FedRAMP ATO. While both the Salesforce commercial cloud and the Salesforce Government Cloud implement similar security controls, only the Salesforce Government Cloud has been assessed against NIST SP 800-53 controls by an independent third party and only the Salesforce Government Cloud maintains a FedRAMP Moderate ATO. Please contact your Salesforce Account Executive to discuss other compliance frameworks or privacy regulations, including those at the state and local levels, which are not covered by the FedRAMP Moderate baseline or DoD IL4 requirements.

Government Contractors

Government contractors may utilize commercial CSOs for a variety of use cases. Depending on the use case and the sensitivity of data managed by a commercial CSO, Government-mandated compliance frameworks may be relevant.

Per DFARS 252.204-7012, contractors using an external cloud service provider (CSP) for internal business purposes to store, process, or transmit Covered Defense Information (CDI) must require and ensure the CSO meets security requirements equivalent to those established by the FedRAMP Moderate baseline.

Per DFARS 252.239-7010, contractors must adhere to the DoD CC SRG when operating a cloud-based system on behalf of the Government in performance of a DoD contract.

The Salesforce Government Cloud has been assessed by a 3PAO against both the FedRAMP Moderate and DoD CC SRG IL4 baselines and maintains a FedRAMP Moderate ATO and IL2 / IL4 PAs.

Conclusion: Government Organizations and Contractors Trust Salesforce

Salesforce recognizes and appreciates that government solutions need to address specific high-priority security requirements. We will continue to partner with governments at all levels to demonstrate that the required level of protection can be provided in the cloud environment. For more detailed information on Salesforce's security for the Salesforce Government Cloud, please contact your Salesforce Account Executive.

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 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/.