CMMC & Salesforce Offerings

Safeguarding CUI with FedRAMP Authorized Cloud Services

Table of Contents

Overview

Salesforce is committed to the success of our customers and to ensuring our customers can continue to use our services to meet their mission and be enabled to comply with applicable data protection laws. Driven by our shared security and compliance responsibility model, compliance with data protection laws requires transparency from Salesforce with our customers in their use of our services. As part of our commitment to our customers, we've published this document to describe the Salesforce features customers can use when storing, processing, or managing Controlled Unclassified Information (CUI), and to assist our customers in documenting their compliance with the U.S. Department of Defense's (DoD) Cybersecurity Maturity Model Certification (CMMC).

The approach discussed in this document includes the following benefits:

- Enables the organization to comply with ever-evolving cybersecurity requirements by using a Cloud Service Provider (CSP), such as Salesforce;
- Provides a secure platform to help drive our customer's digital transformation with a suite of capabilities for existing and new application development; and
- Removes significant technical burden from Government Contractors allowing them to focus less on CMMC compliance and more on their business functions and mission.

In addition to further articulating these benefits, this white paper provides background on CMMC, discusses some of the challenges associated with protecting CUI, and explains how Salesforce can help Government Contractors achieve CMMC compliance with offerings like Salesforce Government Cloud, Salesforce Government Cloud Plus, MuleSoft Government Cloud, and Shield, which have all been used by Government Contractors and the DoD itself for years to secure sensitive unclassified data.

CMMC Background

The Defense Industrial Base (DIB) and the DoD supply chain are critical elements of the DoD and its mission areas. Accordingly, U.S. Government Contractors have been targets of malicious cyber actors, including foreign nation states and rogue entities, which leads to increased risk to national security and impacts the reputation and financial stability of targeted entities. To protect sensitive unclassified Defense information, including Federal Contract Information (FCI) and CUI, along with the intellectual property of DIB organizations, and ensure the rapid reporting of cyber incidents, DoD developed CMMC, which defines processes and practices for cybersecurity across five maturity levels as shown in Figure 1.

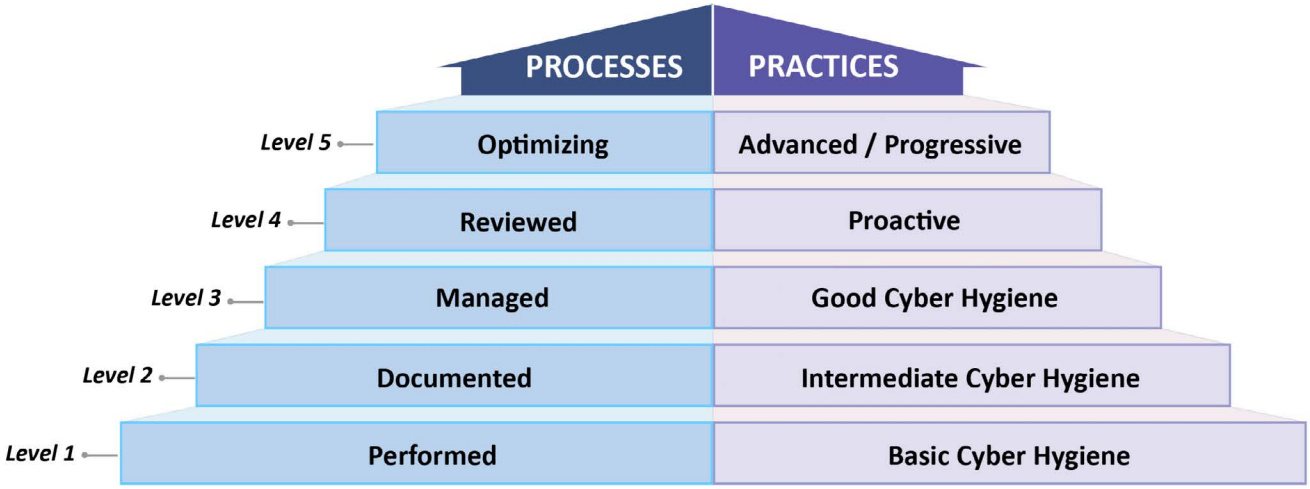

Figure 1: CMMC Levels, Processes, and Practices[1]

While effective cybersecurity is in every organization's best interest, this standardized approach to defense across a global contractor base consisting of 300,000+ organizations creates additional burden for impacted companies, as compliance is required to bid on and participate in all future Defense contracts.

Challenges Protecting CUI

In coordination with the DoD, Defense prime contractors and subcontractors, have long had the responsibility to protect sensitive unclassified data. In recent years, that responsibility has expanded into a series of Defense Federal Acquisition Regulation Supplement (DFARS) clauses, culminating with CMMC. As the threat landscape has evolved, the associated cybersecurity requirements have maintained pace, yielding a moving target for DIB organizations. Due to the nature of cybersecurity, future ongoing evolution should be anticipated.

1. Source: https://www.acq.osd.mil/cmmc/docs/CMMC_v1.0_Public_Briefing_20200131_v2.pdf

And while DoD has announced a phased rollout for CMMC occurring over fiscal years 2021-2025, Government Contractors may reduce their acquisition risk by targeting a CMMC level at or beyond anticipated contract requirements in the near term. It is estimated that 20% of the DIB will require Level 3[2], or higher, to protect CUI, however, a significant percentage of organizations are aiming for Level 3 to maintain their competitive advantage within the industry. In short, Government Contractors are seeking the highest levels of security today, not tomorrow.

In short, Government Contractors are seeking the highest levels of security today, not tomorrow.

Protecting CUI with Salesforce

At Salesforce, trust is our #1 value. Many of our customers operate in regulated industries of financial services, healthcare, government, and, of course, national defense. Earning the trust of our customers in the U.S. Government and national defense industries requires that we address the safeguards and requirements outlined by DFARS 252.204-7000[3] for securing Covered Defense Information (CDI), including CUI.

Leveraging a FedRAMP authorized Cloud Service Offering (CSO) to protect CUI and achieve CMMC compliance is optimized by using an authorized Software as a Service (SaaS) or low-code Platform as a Service (PaaS).

As industry awaits official reciprocity guidance for the Federal Risk and Authorization Management Program (FedRAMP)[4] from DoD, we have positioned ourselves to help our customers meet compliance requirements for their in-scope information systems driven by our existing FedRAMP and DoD authorizations. According to a DoD representative, CMMC Level 3 is equivalent to FedRAMP Moderate.[5] Today, Salesforce meets or exceeds this level of FedRAMP authorization with our U.S. Government offerings, as described on the Salesforce Compliance Portal.

Leveraging a FedRAMP authorized Cloud Service Offering (CSO) to protect CUI and achieve CMMC compliance is optimized by using an authorized Software as a Service (SaaS) or low-code Platform as a Service (PaaS). The benefits of this approach include:

- Helps reduce ongoing risk and cost for the organization associated with the likely ever evolving cybersecurity requirements by shifting significant responsibly to the CSP
  - › As the threat landscape evolves, so too do mitigating security controls. While DoD and NIST have

2. Source: https://federalnewsnetwork.com/reporters-notebook-jason-miller/2021/02/cmmc-update-pilots-3paos-and-more-of-what-vendors-need-to-know/
3. DFARS 252.204-7000 Disclosure of Information: https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm
4. https://fcw.com/articles/2021/02/11/cmmc-reciprocity-fedramp-dibcac.aspx
5. Source: https://www.nextgov.com/cybersecurity/2021/01/official-reciprocity-memos-dods-cybersecurity-certification-program-are-ready/171680/

provided a baseline for required security controls, organizations should assume those controls will change over time. This will lead to ever-increasing total cost of ownership (TCO) of information systems.

  - CSPs who offer FedRAMP and DoD authorized CSOs, such as the services within the authorization boundaries of Salesforce Government Cloud, Salesforce Government Cloud Plus, and Mulesoft Government Cloud, as described on the FedRAMP Marketplace, have invested heavily in this market and must continue to maintain ongoing compliance with relevant security frameworks.

- Provides a secure platform to help drive our customer's digital transformation with a suite of capabilities for existing and new application development
  - With point and click application and page builders, which can include workflows, approvals, and process automation, organizations can quickly configure Salesforce to support their complex business processes.
  - Three Salesforce updates a year are made automatically available to all customers, ensuring ongoing innovation.
  - Built in reporting and analytics allow you to quickly identify trends and patterns for data both internal and external to the platform.
  - Secure, centralized management of APIs and integrations to simplify enterprise system development.
  - The Salesforce AppExchange is the marketplace for all things Salesforce – Whether it be an app for contract management, electronic signatures, or tracking security and compliance, third party independent software vendors (ISVs) have got you covered.[6]
- Removes significant technical burden from Government Contractors allowing them to focus less on CMMC compliance and more on their business functions and mission
  - Initial control implementation, self-assessment, and eventual third party assessment of information systems will be costly and time-consuming endeavors for Government Contractors.
  - Anticipated FedRAMP reciprocity allows Government Contractors to significantly reduce those efforts.
  - Control inheritance is optimized by deploying or building apps with a FedRAMP authorized PaaS / SaaS as described in the following section and depicted in Figure 2.

The Salesforce shared security and compliance responsibility model, our dedicated U.S. Government environments, and Salesforce Shield provide Government Contractors a rapid path to achieve these benefits and CMMC compliance.

Optimized PaaS/SaaS Shared Security and Compliance Responsibility Model

With Salesforce PaaS and SaaS, ensuring data security and compliance is a shared responsibility with customers. While Salesforce provides secure and FedRAMP-compliant services to help protect customer data and applications, customers are ultimately responsible for properly configuring and operating those services as required by their organization and the compliance requirements by which they are bound.

6. To understand how AppExchange components might impact CMMC compliance see this help article.

As depicted in Figure 2, 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 slow ongoing IT modernization. It can also introduce risk and impact compliance. To protect CUI, and ultimately comply with CMMC Levels 3 and higher, this means organizations must implement and maintain at least 130 practices, or controls, across the 17 CMMC domains.

While Infrastructure as a Service (IaaS) may alleviate some burden (e.g. Physical Protection practices), organizations are still responsible for deploying software to the environment, configuring that software, maintaining the software (i.e. patch and upgrade), worrying about dependencies within the stack, and independently implementing the majority of CMMC practices. Accordingly, deploying applications to an IaaS yields minimal risk reduction.

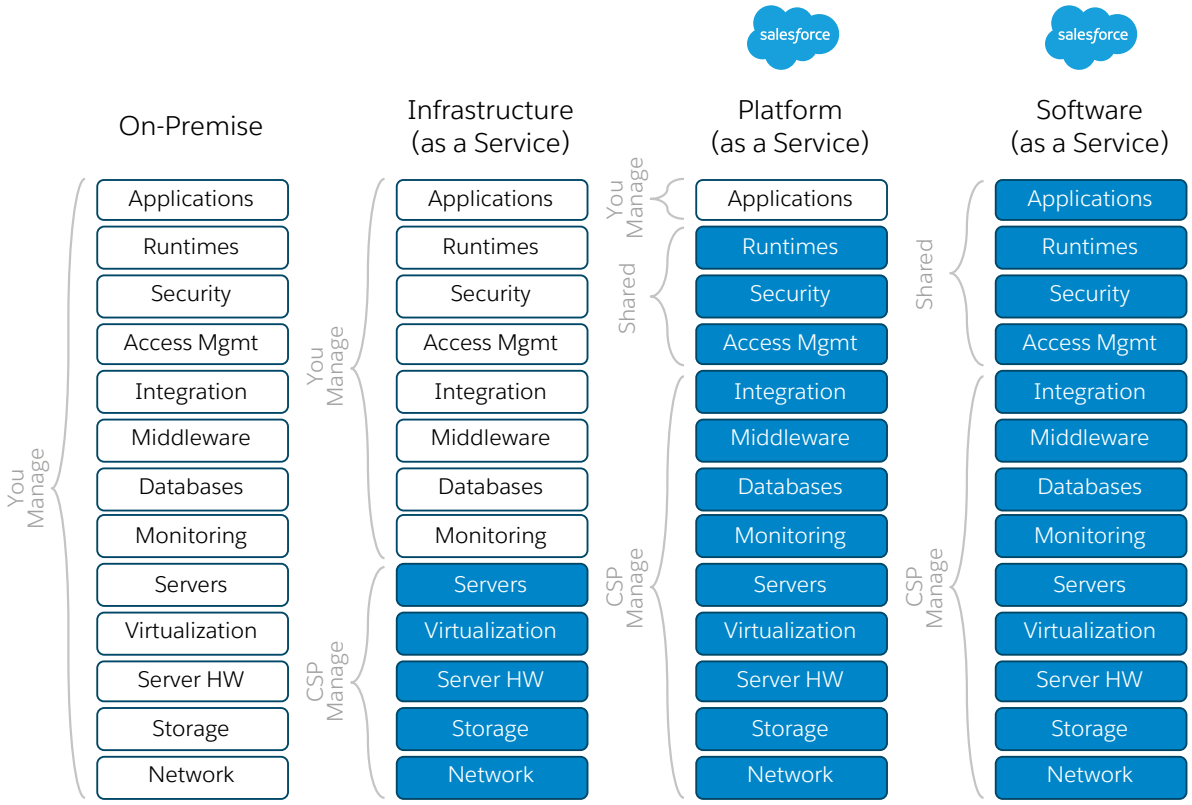

Figure 2: Delivery Models

With Salesforce, customers inherit the majority of security controls. While Defense Contractors bear ultimate responsibility for ensuring security and compliance, Salesforce provides numerous enablement resources, including training and implementation guides. Specifically, for customers seeking compliance with NIST SP 800-171 and CMMC, Salesforce provides a System Security Plan and Customer Responsibility Matrix which address FedRAMP controls that map to those frameworks. This shared responsibility model greatly reduces both risk and burden for customers, allowing them to place more focus on their business and mission.

Dedicated U.S. Government Environments

Salesforce Government Cloud, Government Cloud Plus, and MuleSoft Government Cloud are dedicated instances of Salesforce's industry-leading PaaS and SaaS offerings designed to address the stringent security and compliance requirements of U.S. Government agencies, U.S. Government Contractors, and Federally Funded Research and Development Centers (FFRDCs). While isolated from commercial Salesforce Services and MuleSoft instances, the underlying architectures are the same trusted architecture models that support Salesforce's public cloud offerings and billions of customer transactions a day. These dedicated instances are deployed to U.S. data centers, with all management provided by U.S.-based U.S. citizens. Furthermore, encryption for data at rest and in transit is FIPS 140-2 validated and all environments either meet or exceed requirements of the FedRAMP Moderate control baseline.

Salesforce Government Cloud, Government Cloud Plus, and MuleSoft Government Cloud are dedicated instances of Salesforce's industry-leading PaaS and SaaS.

Salesforce Government Cloud

In 2014, Salesforce obtained FedRAMP authorization for both PaaS and SaaS with Salesforce Government Cloud. Later in 2017, Salesforce Government Cloud was added to the DoD Cloud Computing Catalog after being granted Impact Level 4 (IL4) authorization. Since that time, countless DoD agencies and U.S. Government Contractors have rapidly deployed applications managing CUI with Salesforce Government Cloud in a secure and compliant manner.

Salesforce Government Cloud maintains the following relevant authorizations and certifications. For more, visit https://compliance.salesforce.com/en/services/government-cloud.

- FedRAMP Moderate Agency Authority to Operate (ATO)
- DoD IL2 Provisional Authorization (PA)
- DoD IL4 PA
- NIST SP 800-171 attestation

Salesforce Government Cloud Plus

In 2020, Salesforce launched Government Cloud Plus, providing U.S. Government customers with enhanced security and compliance controls. Running on AWS GovCloud, Salesforce Government Cloud Plus offers end-to-end encryption and is authorized at the FedRAMP High impact level.

Salesforce Government Cloud Plus maintains the following relevant authorizations and certifications. For more, visit https://compliance.salesforce.com/en/services/government-cloud-plus.

- FedRAMP High Joint Authorization Board (JAB) ATO
- DoD IL2 PA
- NIST SP 800-171 attestation

MuleSoft Government Cloud

In 2019, MuleSoft Government Cloud was authorized as a FedRAMP-compliant cloud deployment of the Anypoint Platform, providing the U.S. Government with a secure integration Platform as a Service (iPaaS).

MuleSoft Government Cloud maintains the following relevant authorizations and certifications. For more, visit https://compliance.salesforce.com/en/services/mulesoft-government-cloud.

- FedRAMP Moderate Agency ATO
- DoD IL2 PA
- Implementation of NIST SP 800-171 controls[7]

Salesforce Shield

Salesforce offers a premium set of features built natively on the Salesforce Platform that customers with complex security, governance, and compliance needs can choose to leverage. These services – Field Audit Trail, Event Monitoring, and Platform Encryption – are available via the Salesforce Shield product offering, which provides flexible and configurable capabilities for enhanced protection, monitoring, and retention of your critical data stored in Salesforce. For additional information on Shield, please refer to the Salesforce Shield White Paper.

7. As documented in NIST SP 800-171, Appendix D, the required NIST SP 800-53 controls are a subset of those required by the FedRAMP Moderate control baseline

Field Audit Trail

In the case of a cyber incident, Government Contractors must provide forensics data to DoD to meet CMMC requirements. Field Audit Trail can help meet this requirement by giving a customer up to ten years of audit trail data for up to sixty fields per object. This expands what is currently available to a customer via the Field History Retention feature. With this, a customer can review the historical state and value of their data over a 10 year period and identify who changed it and when.

Know the state and value of your data going back up to 10 years.

Event Monitoring

As required by CMMC, audit logs must be maintained for monitoring, analysis, investigation, and reporting of unlawful or unauthorized activity, and actions must be uniquely traceable to users. Event Monitoring gives Government Contractors visibility into what data users are accessing, from what IP address, and what actions are being taken in regards to that data. Customers utilizing this feature can access event logs and real-time event streams via an application programming interface (API) and can pull the data into any number of visualization tools including, for example, Tableau CRM or third party tools. This feature could enable a customer to track when a page or list view is printed, a record is edited or created, ownership of a record is changed, a list is refreshed, or even when a user exports data. Event Monitoring may be helpful to a customer responding to data audits or identifying and analyzing a potential cyber incident. Together with Event Monitoring, Transaction Security – a framework that intercepts a subset of real-time Salesforce events (e.g., logins, data exports, report access) – can be leveraged to apply appropriate actions like requiring a second factor of authentication, blocking the action entirely and/or notifying an administrator based on security policies you create. This functionality can be used to prevent a potential cyber incident.

Monitor user activity and create real-time security policies to prevent and/or track undesired activity.

Platform Encryption

Platform Encryption enables Government Contractors to encrypt sensitive data at rest, including CUI, at the platform level with FIPS-validated cryptography, which is required by CMMC, while maintaining important application functionality–(i.e., search, validation, workflow, etc.). Given that data is encrypted at the metadata layer in the database, key Salesforce application functionality can be made "encryption aware" and work despite the data being encrypted. With Platform Encryption, customers are able to render sensitive data unreadable by unauthorized persons. Additionally, customers are provided multiple options to manage the encryption key lifecycle. In the event of a data spill, this functionality can allow a customer to cryptographically erase the offending data from Salesforce.

Encrypt sensitive data at rest, including CUI, at the platform level, and manage encryption keys.

Conclusion

The trust and success of our customers are the highest priorities for Salesforce. As a CSP vested in the U.S. Government market for over a decade, and one who has helped countless DoD agencies and Government Contractors protect CUI for years, Salesforce is committed to transparency with our customers to help them safeguard sensitive U.S. Government data along with their own intellectual property. For more on how we do this today, reach out to your Salesforce account executive and visit https://www.salesforce.com/government. Or, to identify a Salesforce Government Solution Expert, visit https://www.salesforce.com/form/industries/government/government-solution-expert/.

Document Disclaimer

About Salesforce

Salesforce transforms government agencies and their industry partners into highly connected, efficient, and productive organizations. The Salesforce Platform accelerates transformation to deploy solutions with a multi-tenant cloud infrastructure that meets security and compliance requirements. To learn more, visit www.salesforce.com/government or call (844) 807-8829 to speak to a government expert