

# Moderately Confused: Decoding FedRAMP Equivalence for Defense Contractors

Scott Sawyer

Co-Founder & Chief Scientist

# About Scott & Paperless Parts

## Co-Founder & Chief Scientist

- Electrical engineer by training
- R&D engineer in the defense industry (Lockheed Martin & MIT Lincoln Laboratory)
- VP Engineering at consumer electronics startup
- Started Paperless Parts in 2017
- Focused on core technology & innovation
- *Not a lawyer, doctor, assessor, RP, sysadmin, or tax accountant*

## Paperless Parts

- Cloud-native quoting and estimating software for manufacturers
- Typical customer profile includes US machine shops, sheet metal fabricators, and additive service bureaus
- Analyze technical data (3D models and 2D drawings) for manufacturability and costing
  - Collaborate internally and externally in context
- Founding team has deep roots in defense



PART 90  
REV ---  
24mm-simple-plate.step



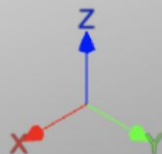
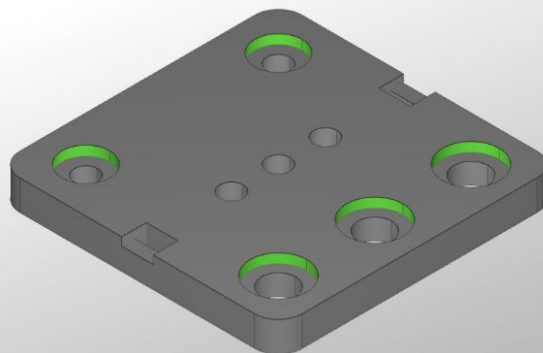
CAD

PART NUMBER  
90

REVISION  
---

PROCESS TYPE  
Sheet Metal

MATERIAL  
---



Tree Geometric Features

GEOMETRIC ANALYSIS [Edit](#)  
Default Sheet Metal (Laser)

- SHEET METAL FEATURES
- Counterbore (5) ⓘ
  - Cutout Feature (4)
  - Simple Drilled Hole (5) ⓘ

23 MANUFACTURING WARNINGS

File Properties  
Volume: 1.242 cu. in  
Area: 14.581 sq. in  
Weight: ---

Team  
EXPIRES AT 1/1/22 12:40PM

12:40 PM, OCT 29 2021  
Donna To shared this channel with donna.to+customer@paperlessparts.com from Tessellate Customer.

Donna To 2:59 PM, DEC 14 2021  
Thanks for sending this over, can we change the material for AU 6061-T6? @Donna Customer  
[Reply](#) [Edit](#) [Delete](#)

Donna To 2:59 PM, DEC 14 2021  
Features (5)  
Counterbore (5) ⓘ

Will this require special tooling?  
[Reply](#) [Edit](#) [Delete](#)

Add Message [Tag Teammate](#) [Add Annotation](#)



# Agenda

- Regulatory Context
- FedRAMP Overview
- “The Memo”
- An Approach to Evaluating Vendors



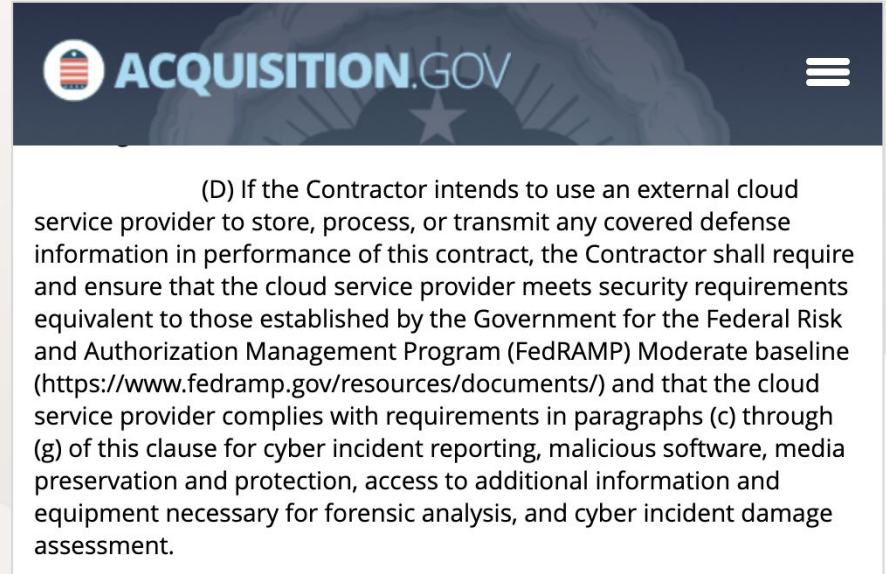
# Agenda

- Regulatory Context
- FedRAMP Overview
- “The Memo”
- An Approach to Evaluating Vendors

# In The Beginning

...there was DFARS 252.204-7012 (b)(2)(ii)(D)

- Applies to Cloud Service Providers (CSPs) used to store, process, or transmit covered data
- Imposes security requirements above and beyond CMMC L2 (“FedRAMP Moderate”):
  - ~3x the number of controls
  - ~4x the number of determination statements
- (c) through (g) relate to incident response and reporting
- “equivalent to,” you say?



# Three Categories of Requirements for CSPs Emerge



FedRAMP

1. Implement security requirements equivalent to the FedRAMP Moderate baseline and use US-based infrastructure.



2. Agree to support DOD incident response requirements.



3. If any information will be export controlled, ensure all CSP staff with access to customer data are US Persons.

# Finding a Low-Risk Path Forward

## CSP Perspective (2018-2023)

Proceed as if pursuing FedRAMP Authority to Operate:

- Adopt FedRAMP Moderate as baseline for SSP.
- Retain top two FedRAMP-recognized 3PAOs for advisory and assessment, respectively.
- Hire US Persons for roles requiring privileged access. Maintain ITAR registration.
- Host all infrastructure on AWS GovCloud and use other FedRAMP services.
- Define and document a shared responsibility model (Customer Responsibility Matrix).
- Resource with multi-million dollar budget.





# Assessing Use of Cloud Service Providers

## July 2022: CMMC Assessment Process (Pre-Decisional Draft)

### 2.2.4 Determine FedRAMP Moderate Equivalency for Cloud Computing Providers

If the OSC is utilizing a Supporting Organization that is an External Cloud Service Provider, the C3PAO Assessment Team will be responsible for ascertaining and determining if the External Cloud Service Provider meets the security requirements “equivalent” to the FedRAMP Moderate baseline as per the DFARS 252-204-7012(b)(2)(ii)(D) requirement.

The OSC can ensure that the External Cloud Service Provider meets security requirements equivalent to FedRAMP Moderate in the same way the OSC would normally ensure any services or product being contracted for will meet its requirements. For example, an External Cloud Service Provider may choose to provide evidence that it meets the security requirements equivalent to FedRAMP Moderate by providing a body of evidence (BOE) that attests to and describes how the External Cloud Service Provider meets the FedRAMP Moderate baseline security requirements.

Examples of items that could be included in such a BOE are an SSP that describes the system environment, system responsibilities, and the current status of the FedRAMP Moderate baseline controls required for the system, as well as a Customer Implementation Summary/Customer Responsibility Matrix that summarizes how each control is met and which party is responsible for maintaining that control.

- CSP has a Body of Evidence (BOE), which may or may not include specific FedRAMP-required documents.
- BOE has been attested to by a qualified source.
- CMMC assessor is not expected to conduct a “quasi-FedRAMP” assessment.

In determining whether the External Cloud Service Provider meets the FedRAMP moderate “equivalency” requirement, the C3PAO Assessment Team shall examine whether the OSC has met the following two criteria:

- 1) The OSC or the External Cloud Service Provider has provided a body of evidence documenting how the External Cloud Service Provider’s security controls are equivalent to those provided by the FedRAMP Moderate baseline standard; and
- 2) Said body of evidence has been attested to by an independent, credible, professional source.

If the C3PAO Assessment Team’s examination concludes that both criteria have been met, the OSC’s External Cloud Service Provider can be considered to have met the FedRAMP Moderate equivalency requirement and the C3PAO should consider the DFARS 252-204-7012(b)(2)(ii)(D) requirement satisfied.

If the C3PAO Assessment Team’s examination concludes that both criteria have not been met, then the Assessment findings shall reflect the in-scope CMMC practices for which the External Cloud Service Provider is responsible be scored as NOT MET.

To be clear, the C3PAO Assessment Team **is not** conducting a quasi-FedRAMP certification audit of the External Cloud Service Provider, for which it is neither authorized nor certified. Rather, the C3PAO is applying the two criteria established by DoD to determine if FedRAMP Moderate “equivalency” has been attained and can be recognized.

*Note:* With regard to criterion #2, a CMMC RP or RPO employed, contracted, or under a paid engagement with the OSC may not serve as the independent, credible, professional source for attesting to the FedRAMP Moderate body of evidence. A FedRAMP Third-Party Assessment Organization (3PAO), however, retained by the OSC, may serve in this role to attest to the credibility of the body of evidence.

# Assessing Use of Cloud Service Providers

## December 2023: Proposed Final Rule

(ii) The Cloud Service Provider's (CSP) product or service offering is not FedRAMP Authorized at the FedRAMP Moderate (or higher) baseline but meets security requirements equivalent to those established by the FedRAMP Moderate (or higher) baseline. Equivalency is met if the OSA has the CSP's System Security Plan (SSP) or other security documentation that describes the system environment, system responsibilities, the current status of the Moderate baseline controls required for the system, and a Customer Responsibility Matrix (CRM) that summarizes how each control is MET and which party is responsible for maintaining that control that maps to the NIST SP 800-171 Rev 2

### Federal Register / Vol.

requirements. (See [https://www.fedramp.gov/assets/resources/documents/FedRAMP\\_Moderate\\_Security\\_Controls.xlsx](https://www.fedramp.gov/assets/resources/documents/FedRAMP_Moderate_Security_Controls.xlsx).)

(iii) In accordance with § 170.19, the OSA's on-premises infrastructure connecting to the CSP's product or service offering is part of the CMMC Assessment Scope, which will also be assessed. As such, the security requirements from the CRM must be documented or referred to in the OSA's System Security Plan (SSP).

- CSP has a Body of Evidence (BOE), which may or may not include specific FedRAMP-required documents.
- BOE has been attested to by a qualified source.
- CMMC assessor is not expected to conduct a "quasi-FedRAMP" assessment.
- First mention of Customer Responsibility Matrix (CRM)

# Assessing Use of Cloud Service Providers

## January 2024: FedRAMP Equivalency Memo



**DEPARTMENT OF DEFENSE**  
6000 DEFENSE PENTAGON  
WASHINGTON, D.C. 20301-6000

DEC 21 2023

MEMORANDUM FOR SENIOR PENTAGON LEADERSHIP  
COMMANDERS OF THE COMBATANT COMMANDS  
DEFENSE AGENCY AND DOD FIELD ACTIVITY DIRECTORS

SUBJECT: Federal Risk and Authorization Management Program Moderate Equivalency for  
Cloud Service Provider's Cloud Service Offerings

References: (a) Federal Risk and Authorization Management Program,  
<https://www.fedramp.gov/>

- BOE must be a proper FedRAMP package including 20+ required documents (SSP, CRM, policies, and more)
- Assessment and attestation from recognized FedRAMP 3PAO
- “100% compliant”



# Agenda

- Regulatory Context
- FedRAMP Overview
- “The Memo”
- An Approach to Evaluating Vendors



# Agenda

- Regulatory Context
- FedRAMP Overview
- “The Memo”
- An Approach to Evaluating Vendors

# Federal Risk and Authorization Management Program

## What is FedRAMP?

- **Process through which federal agencies accept the risk associated with using a cloud service.**
- Based on NIST SP 800-53, the standard from which 800-171 is tailored.
- Controls selected for different baselines (Low, Moderate, High) based on sensitivity of the data handled.
- Once one agency authorizes, additional agencies can adopt more easily.



FedRAMP

# Controls & Baselines

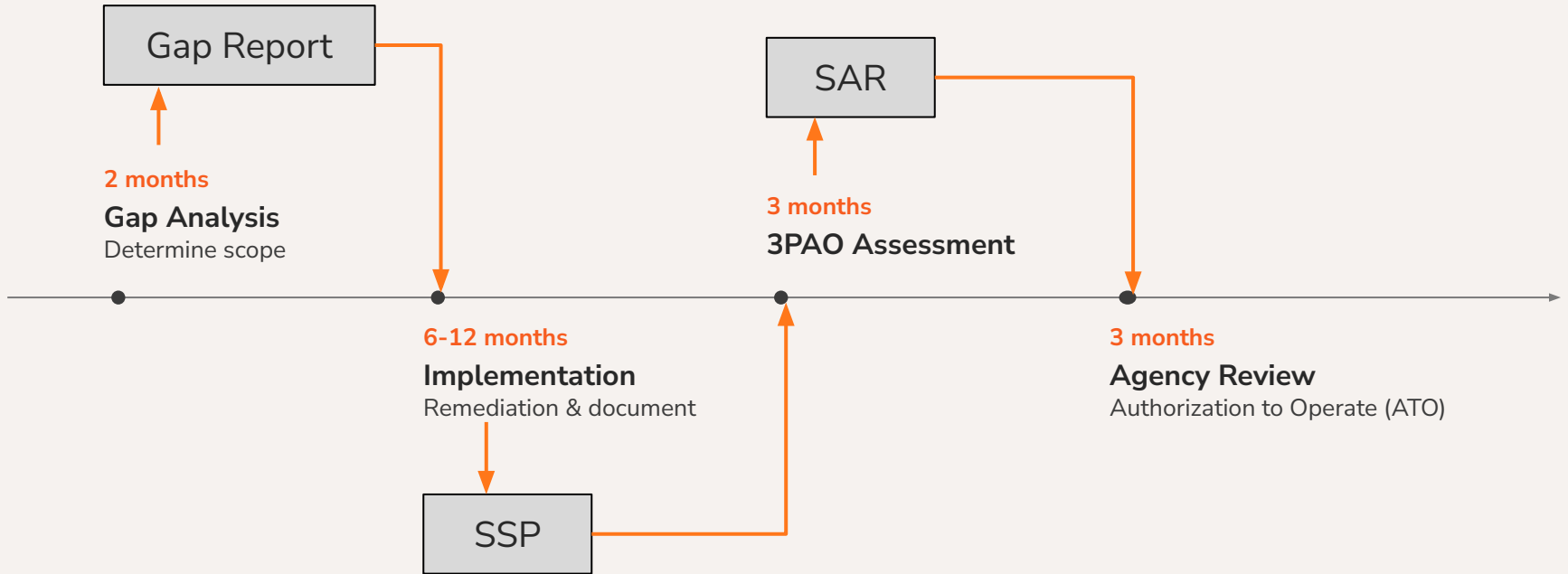
## 800-53 Baselines and Additional FedRAMP Requirements

ID	Control Name	H FedRAMP-Defined Assignment / Selection Parameters	H Additional FedRAMP Requirements and Guidance
AC-1	Policy and Procedures	AC-1 (c) (1) [at least annually] AC-1 (c) (2) [at least annually] [significant changes]	
AC-2	Account Management	AC-2 (h) (1) [twenty-four (24) hours] AC-2 (h) (2) [eight (8) hours] AC-2 (h) (3) [eight (8) hours] AC-2 (j) [monthly for privileged accessed, every six (6) months for non-privileged access]	

## Moderate Control Examples

- NIST 800-171 is a subset.
- Additional requirement examples:
  - Continuous scanning and monitoring
  - Penetration testing
  - Physical resilience
  - Secure software development
- FedRAMP is in transition from Rev 4 to Rev 5.

# Typical FedRAMP Authorization Timeline





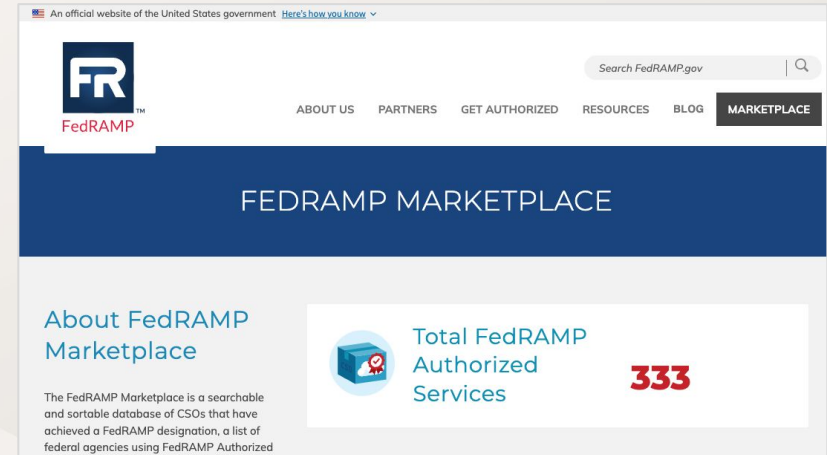
# Authorization

## Requires Government Customer(s)

Risk can be accepted by an individual agency purchasing the cloud service or by a Joint Authorization Board (JAB).

JAB reviews 10-12 services per year and prioritizes based on widespread use within the government (capacity largely consumed by Microsoft, Amazon, and Google).

Once Authorized, services appear in the FedRAMP.gov Marketplace, for other agencies to find them.





# Agenda

- Regulatory Context
- FedRAMP Overview
- “The Memo”
- An Approach to Evaluating Vendors



# Agenda

- Regulatory Context
- FedRAMP Overview
- “The Memo”
- An Approach to Evaluating Vendors

# The Importance of Equivalency

## The DIB Relies on Industry-Specific Software

- The cloud has won for many reasons.
- DIB contractors need to communicate, quote, manufacture, and deliver the supplies the DOD needs to execute the mission.
- The FedRAMP Marketplace does not include industry-specific tools.

## Examples

- Computer Aided Design (CAD) & 3D Viewers
- Computer Aided Manufacturing (CAM)
- Simulation
- Configure/Price/Quote (CPQ)
- Manufacturing Execution/Planning Systems (ERP/MES/MRP)
- Machine Tools & Monitoring
- Quality

# Memorandum on FedRAMP Equivalency

December 21, 2023 / Released January 2, 2024

# Memorandum on FedRAMP Equivalency

December 21, 2023 / Released January 2, 2024

## System Security Plan (SSP)

- Information Security Policies and Procedures (covering all control families)
- User Guide
- Digital Identity Worksheet
- Rules of Behavior (RoB)
- Information System Contingency Plan (ISCP)
- Incident Response Plan (IRP)
- Configuration Management Plan (CMP)

**CLEARED  
For Open Publication**

Jan 02, 2024

Department of Defense  
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

- Control Implementation Summary (CIS) Workbook
- Federal Information Processing Standard (FIPS) 199
- Separation of Duties Matrix
- Applicable Laws, Regulations, and Standards
- Integrated Inventory Workbook

## Security Assessment Plan (SAP)

- Security Test Case Procedures
- Penetration Testing Plan and Methodology conducted annually and validated by a FedRAMP-recognized Third Party Assessment Organization (3PAO)
- FedRAMP-recognized 3PAO Supplied Deliverables (e.g., Penetration Test Rules of Engagement, Sampling Methodology)

## Security Assessment Report (SAR) performed by a FedRAMP-recognized 3PAO

- Risk Exposure Table
- Security Test Case Procedures
- Infrastructure Scan Results conducted monthly and validated annually by 3PAO
- Database Scan Results conducted monthly and validated annually by a FedRAMP-recognized 3PAO
- Web Scan Results conducted monthly and validated annually by a FedRAMP-recognized 3PAO
- Auxiliary Documents (e.g., evidence artifacts)
- Penetration Test Reports

## Plan of Action and Milestones (POA&M)

- Continuous Monitoring Strategy (required by CA-7)
- Continuous Monitoring Monthly Executive Summary, validated annually by a FedRAMP-recognized 3PAO

# Memorandum on FedRAMP Equivalency

December 21, 2023 / Released January 2, 2024

## System Security Plan (SSP)

- Information Security Policies and Procedures (covering all control families)
- User Guide
- Digital Identity Worksheet
- Rules of Behavior (RoB)
- Information System Contingency Plan (ISCP)
- Incident Response Plan (IRP)
- Configuration Management Plan (CMP)

**CLEARED  
For Open Publication**

Jan 02, 2024

Department of Defense  
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

DoD requirements for FedRAMP Moderate Equivalency do not allow for POA&M's resulting from a 3PAO assessment of the CSP's CSO. All POA&M actions must be corrected and validated by the 3PAO as closed. CSPs are allowed to have operational POA&Ms which are not the result of FedRAMP-recognized 3PAO assessment.

- Control Implementation Summary (CIS) Workbook
- Federal Information Processing Standard (FIPS) 199
- Separation of Duties Matrix
- Applicable Laws, Regulations, and Standards
- Integrated Inventory Workbook

## Security Assessment Plan (SAP)

- Security Test Case Procedures
- Penetration Testing Plan and Methodology conducted annually and validated by a FedRAMP-recognized Third Party Assessment Organization (3PAO)
- FedRAMP-recognized 3PAO Supplied Deliverables (e.g., Penetration Test Rules of Engagement, Sampling Methodology)

## Security Assessment Report (SAR) performed by a FedRAMP-recognized 3PAO

- Risk Exposure Table
- Security Test Case Procedures
- Infrastructure Scan Results conducted monthly and validated annually by 3PAO
- Database Scan Results conducted monthly and validated annually by a FedRAMP-recognized 3PAO
- Web Scan Results conducted monthly and validated annually by a FedRAMP-recognized 3PAO
- Auxiliary Documents (e.g., evidence artifacts)
- Penetration Test Reports

## Plan of Action and Milestones (POA&M)

- Continuous Monitoring Strategy (required by CA-7)
- Continuous Monitoring Monthly Executive Summary, validated annually by a FedRAMP-recognized 3PAO

# Memorandum on FedRAMP Equivalency

December 21, 2023 / Released January 2, 2024

## System Security Plan (SSP)

- Information Security Policies and Procedures (covering all control families)
- User Guide
- Digital Identity Worksheet
- Rules of Behavior (RoB)
- Information System Contingency Plan (ISCP)
- Incident Response Plan (IRP)
- Configuration Management Plan (CMP)

**CLEARED  
For Open Publication**

Jan 02, 2024

Department of Defense  
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

DoD requirements for FedRAMP Moderate Equivalency do not allow for POA&M's resulting from a 3PAO assessment of the CSP's CSO. All POA&M actions must be corrected and validated by the 3PAO as closed. CSPs are allowed to have operational POA&Ms which are not the result of FedRAMP-recognized 3PAO assessment.

The contractor acts as approver for the use of the CSO by their organization and confirms that the selected CSP has an incident response plan. The contractor, not the CSO's CSP, will be held responsible for reporting in the event of CSO compromise. The contractor shall ensure the CSP follows the incident response plan and can provide notifications to the contractor. The contractor will report incidents in accordance with the applicable contract terms and conditions.

- Control Implementation Summary (CIS) Workbook
- Federal Information Processing Standard (FIPS) 199
- Separation of Duties Matrix
- Applicable Laws, Regulations, and Standards
- Integrated Inventory Workbook

## Security Assessment Plan (SAP)

- Security Test Case Procedures
- Penetration Testing Plan and Methodology conducted annually and validated by a FedRAMP-recognized Third Party Assessment Organization (3PAO)
- FedRAMP-recognized 3PAO Supplied Deliverables (e.g., Penetration Test Rules of Engagement, Sampling Methodology)

## Security Assessment Report (SAR) performed by a FedRAMP-recognized 3PAO

- Risk Exposure Table
- Security Test Case Procedures
- Infrastructure Scan Results conducted monthly and validated annually by 3PAO
- Database Scan Results conducted monthly and validated annually by a FedRAMP-recognized 3PAO
- Web Scan Results conducted monthly and validated annually by a FedRAMP-recognized 3PAO
- Auxiliary Documents (e.g., evidence artifacts)
- Penetration Test Reports

## Plan of Action and Milestones (POA&M)

- Continuous Monitoring Strategy (required by CA-7)
- Continuous Monitoring Monthly Executive Summary, validated annually by a FedRAMP-recognized 3PAO



# Memorandum on FedRAMP Equivalency

December 21, 2023 / Released January 2, 2024

## System Security Plan (SSP)

- Information Security Policies and Procedures (covering all control families)
- User Guide
- Digital Identity Worksheet
- Rules of Behavior (RoB)
- Information System Contingency Plan (ISCP)
- Incident Response Plan (IRP)
- Configuration Management Plan (CMP)

**CLEARED  
For Open Publication**

Jan 02, 2024

Department of Defense  
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

DoD requirements for FedRAMP Moderate Equivalency do not allow for POA&M's resulting from a 3PAO assessment of the CSP's CSO. All POA&M actions must be corrected and validated by the 3PAO as closed. CSPs are allowed to have operational POA&Ms which are not the result of FedRAMP-recognized 3PAO assessment.

The contractor acts as approver for the use of the CSO by their organization and confirms that the selected CSP has an incident response plan. The contractor, not the CSO's CSP, will be held responsible for reporting in the event of CSO compromise. The contractor shall ensure the CSP follows the incident response plan and can provide notifications to the contractor. The contractor will report incidents in accordance with the applicable contract terms and conditions.

7020. The onus is on the contractor to validate the BoE provided by the 3PAO meets the Moderate Equivalent standards outlined in this memo and if using a CSO that is FedRAMP Moderate equivalent, must provide the CRM to DIBCAC and 3PAO assessors to support assessments.

- Control Implementation Summary (CIS) Workbook
- Federal Information Processing Standard (FIPS) 199
- Separation of Duties Matrix
- Applicable Laws, Regulations, and Standards
- Integrated Inventory Workbook

## Security Assessment Plan (SAP)

- Security Test Case Procedures
- Penetration Testing Plan and Methodology conducted annually and validated by a FedRAMP-recognized Third Party Assessment Organization (3PAO)
- FedRAMP-recognized 3PAO Supplied Deliverables (e.g., Penetration Test Rules of Engagement, Sampling Methodology)

## Security Assessment Report (SAR) performed by a FedRAMP-recognized 3PAO

- Risk Exposure Table
- Security Test Case Procedures
- Infrastructure Scan Results conducted monthly and validated annually by 3PAO
- Database Scan Results conducted monthly and validated annually by a FedRAMP-recognized 3PAO
- Web Scan Results conducted monthly and validated annually by a FedRAMP-recognized 3PAO
- Auxiliary Documents (e.g., evidence artifacts)
- Penetration Test Reports

## Plan of Action and Milestones (POA&M)

- Continuous Monitoring Strategy (required by CA-7)
- Continuous Monitoring Monthly Executive Summary, validated annually by a FedRAMP-recognized 3PAO



# Agenda

- Regulatory Context
- FedRAMP Overview
- “The Memo”
- An Approach to Evaluating Vendors









# Agenda


- Regulatory Context
- FedRAMP Overview
- “The Memo”
- An Approach to Evaluating Vendors

# Shared Responsibility Model

## Understand the Customer Responsibility Matrix (CRM) Early

		Responsibility			
		SaaS	PaaS	IaaS	On-Prem
 RESPONSIBILITY ALWAYS RETAINED BY CUSTOMER	Information and data	Customer	Customer	Customer	Customer
	Devices (Mobile and PCs)	Customer	Customer	Customer	Customer
	Accounts and identities	Customer	Customer	Customer	Customer
 RESPONSIBILITY VARIES BY TYPE	Identity and directory infrastructure	Shared	Shared	Customer	Customer
	Applications	Microsoft	Shared	Customer	Customer
	Network controls	Microsoft	Shared	Customer	Customer
	Operating system	Microsoft	Microsoft	Customer	Customer
 RESPONSIBILITY ALWAYS TRANSFERS TO CLOUD PROVIDER	Physical hosts	Microsoft	Microsoft	Shared	Customer
	Physical network	Microsoft	Microsoft	Microsoft	Customer
	Physical datacenter	Microsoft	Microsoft	Microsoft	Customer

 Customer    Microsoft    Shared



# Additional Cost for FedRAMP Version

Compliance is big investment, and costs will flow down.

- Developing and operating a FedRAMP Moderate-equivalent SaaS product requires a substantial financial investment.
  - We pay more than \$500K annually in vendor costs alone (plus FTEs!).
- Understand cost and contract structure.
- FedRAMP versions of mass-market products are typically priced 30-50% higher.
  - Government versions may contain fewer features and get less frequent updates.
- Do you handle export controlled data?
  - Ensure the vendor's staff supporting you are US Persons.

# Will Your Vendor Be Ready in Time?

## What to look for in a Body of Evidence

- What's your own deadline for compliance?
- Understand your responsibilities on the Customer Responsibility Matrix.
- POA&M: Ask about solutions and timelines for open items.
- Check Incident Response Policy for government reporting.
- Spot check the SSP for completion of long-lead items.
  - FIPS-validated cryptography (look for certificate numbers)
  - Continuous monitoring: Look for tools like Tenable, SentinelOne, and a SIEM like Splunk or DataDog
- Discussions will put documentation in context.
  - Use Zoom for Government or Teams GCC High when reviewing security documentation.
- **BOE is highly sensitive! Expect tight controls on the documentation.**

# Questions?

Scott Sawyer

[scott@paperlessparts.com](mailto:scott@paperlessparts.com)