

**INFODEFENSE**

# Five Barriers to CMMC Compliance



Kevin Wheeler

Founder & Managing Director

# Why is CMMC so Important?



Lockheed Martin F-35 Lightning



Shenyang FC-31

# CMMC Facts



- ▶ Originally released in January 2020, the Cybersecurity Maturity Model Certification (CMMC) is intended to improve DIB security
- ▶ Based on [NIST SP 800-171](#) which is referenced in [DFARS 252.204-7012](#)
- ▶ Some new contracts may require CMMC certification as soon as 2023
- ▶ All new defense contracts will require CMMC certification in FY 2025

# Don't Wait to Prepare

CMMC Preparation Task	Expertise Required	Estimated Timeline	Date of Completion
Gap Analysis	High	2 Weeks +	April 2023
Plan of Action & Milestones	Medium	2 Months +	June 2023
System Security Plan	High	4 Months +	October 2023
Remediation *	High	<b>12 Months +</b>	October 2024
Evidence Collection	Low	3 Months	<b>January 2025</b>

\* Assuming Low NIST SP 800-171 Compliance Level

# Five Barriers to CMMC Compliance

---

1. Understanding CUI flow
2. Inadequate policies, procedures & compliance related documents
3. Limited security monitoring & incident response capabilities
4. FIPS-compliant vs. FIPS-validated encryption
5. FedRAMP equivalent cloud services

# 1. Understanding CUI Flow

# CUI Flow Analysis

Determine

Determine which business functions support DoD contracts



Identify

Identify processes within each business function where CUI is handled



Map

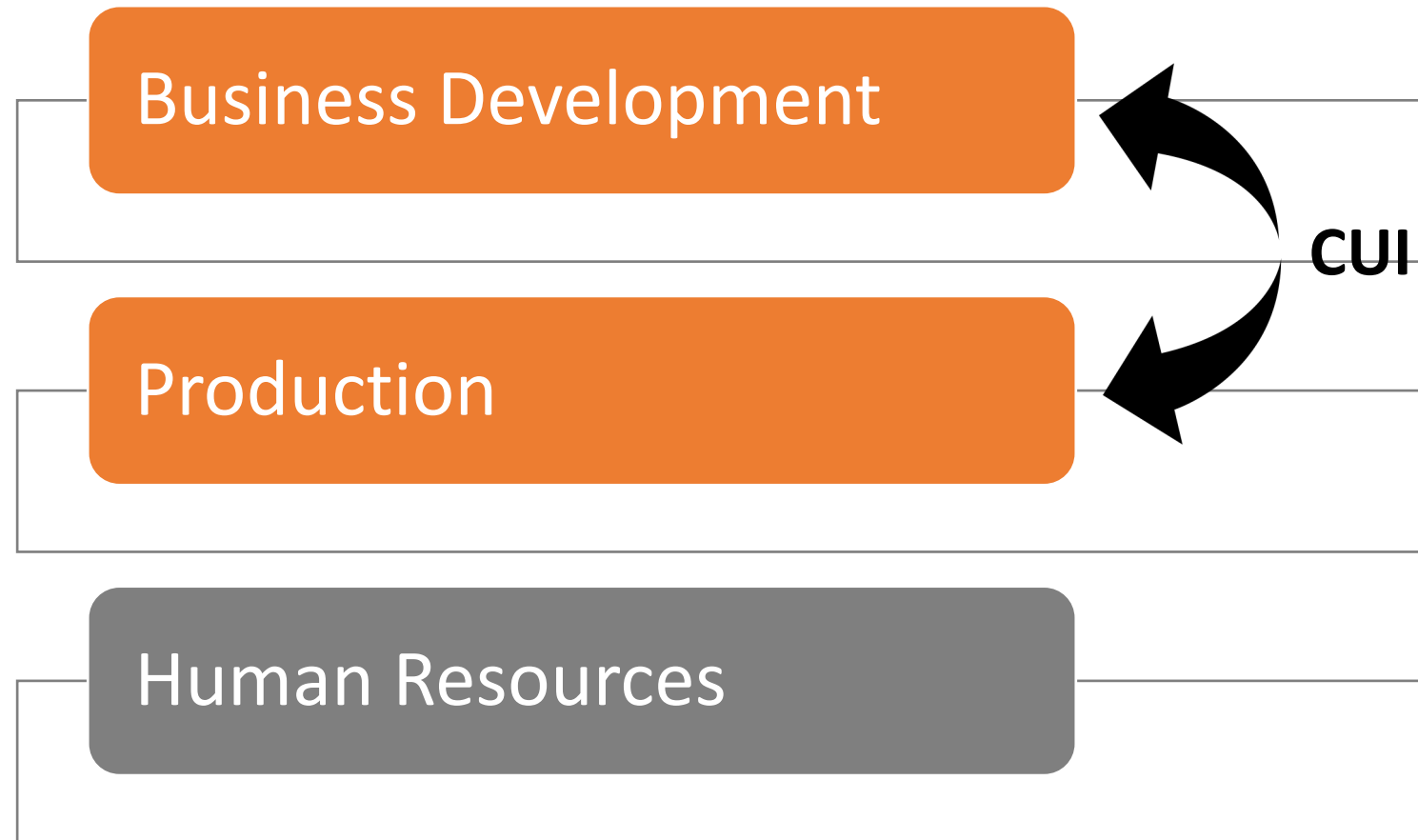
Map the flow of CUI for each business process



Categorize

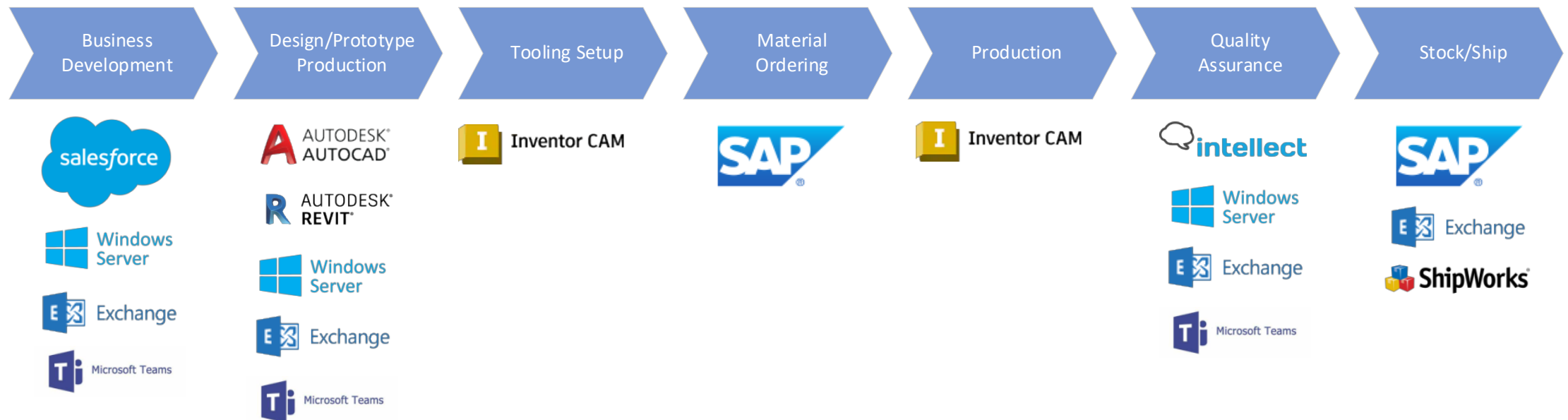
Categorize applications, personnel, networks, systems and facilities

## Business Functions that Handle CUI





# Manufacturing Sales Process



## 2. Inadequate Documentation

## Documents Required for Certification

- System Security Plan (SSP)
- Architecture & CUI flow diagrams
- Policies & procedures that address all requirements
- Security configuration standards
- Incident Response Plan
- Compliance Responsibility Matrix
- Asset Inventory
- Evidence of compliance (artifacts)

# System Security Plan

- **Section 1** – System Identification (Roles, Responsibilities & Contact Information)
- **Section 2** – System Environment (System Architecture, CUI Flow Analysis & CMMC Scope, Overview of Security Controls)
- **Section 3** – CMMC Compliance (Description of how each requirement is met including artifact reference)

[COMPANY NAME] SYSTEM SECURITY PLAN Last Updated: 2/16/23

This System Security Plan was created to provide an account of the controls that have been implemented or will be implemented to protect Controlled Unclassified Information (CUI), Federal Contract Information (FCI) and International Traffic in Arms Regulation (ITAR) information that has been entrusted to [Company Name].

## 1. System Identification

### 1.1. System Name: [Company Name] IT Infrastructure

**System Type(s):** Multi-User Standalone (MUSA) System, Wide Area Network (WAN)

**System Categorization:** Controlled Unclassified Information (CUI), Federal Contract Information (FCI), international Traffic in Arms Regulation (ITAR)

**Information Impact Categorization**

Category	Confidentiality	Integrity	Availability	Authority
CUI	Medium	Low	Low	NARA
FCI	Low	Low	Low	GSA
ITAR	Medium	Low	Low	US Dept. of State

**System Unique Identifier:** [Company Name] IT Infrastructure

**Responsible Organization**  
The following organization is responsible for this System.

Name: \_\_\_\_\_  
Address: \_\_\_\_\_  
Phone: \_\_\_\_\_

**Information Owner**  
The Information Officer is responsible for ensuring the protection of Controlled Unclassified Information (CUI).

Name: \_\_\_\_\_  
Title: \_\_\_\_\_  
Office Address: \_\_\_\_\_  
Work Phone: \_\_\_\_\_  
e-Mail Address: \_\_\_\_\_

**System Owner**  
The System Owner is responsible for applying security controls at a system level to protect CUI according to the requirements defined by the Information Owner.

Name: \_\_\_\_\_  
Title: \_\_\_\_\_

CONFIDENTIAL – LIMITED DISTRIBUTION 3

**Note:** Template can be downloaded from [NIST SP 800-171A](https://www.nist.gov/sp/800-171a) website

# System Security Plan Detail

## Assessment Guidance

<b>3.1.1</b>	<b>SECURITY REQUIREMENT</b> Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).
	<b>ASSESSMENT OBJECTIVE</b> Determine if:
	<b>3.1.1[a]</b> <i>authorized users are identified.</i>
	<b>3.1.1[b]</b> <i>processes acting on behalf of authorized users are identified.</i>
	<b>3.1.1[c]</b> <i>devices (and other systems) authorized to connect to the system are identified.</i>
	<b>3.1.1[d]</b> <i>system access is limited to authorized users.</i>
	<b>3.1.1[e]</b> <i>system access is limited to processes acting on behalf of authorized users.</i>
	<b>3.1.1[f]</b> <i>system access is limited to authorized devices (including other systems).</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b> <b>Examine:</b> [SELECT FROM: Access control policy; procedures addressing account management; system security plan; system design documentation; system configuration settings and associated documentation; list of active system accounts and the name of the individual associated with each account; notifications or records of recently transferred, separated, or terminated employees; list of conditions for group and role membership; list of recently disabled system accounts along with the name of the individual associated with each account; access authorization records; account management compliance reviews; system monitoring records; system audit logs and records; list of devices and systems authorized to connect to organizational systems; other relevant documents or records]. <b>Interview:</b> [SELECT FROM: Personnel with account management responsibilities; system or network administrators; personnel with information security responsibilities]. <b>Test:</b> [SELECT FROM: Organizational processes for managing system accounts; mechanisms for implementing account management].

## System Security Plan

ACME, INC. SYSTEM SECURITY PLAN

Last Updated: 3/14/23

### Access Control (AC) Level 1

**AC.11-3.1.1** - Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

Implemented
  Planned to be Implemented
  Not Applicable

Acme, Inc. has implemented policies, standards and procedures that govern system access control and authorization. End users are issued unique identifiers and are prohibited from sharing passwords. When credentialed system access is necessary, unique identifiers are created for processes acting on behalf of authorized users and devices.

Acme, Inc. utilizes an account request authorization procedure to govern system access. When an account is required for user or system access, a help desk ticket is created to ensure that access provisioning is performed in a consistent manner. Access is granted according to least privilege by role. Manager approval is required prior to the creation of user and system accounts. See the Access Request Procedure for more details.

A list of authorized processes acting on behalf of authorized users and devices is maintained by [IT Service Provider]. End user access is tracked from within Microsoft 365, Active Directory, and other authentication providers. See the System Inventory for a list of authentication providers.

#### Supporting Documents:

ITPC-01 - Access Request Procedure  
 ITPC-01 - Account Provisioning Procedure  
 ITPC-01 - Access Review Procedure

#### Policies and Standards:

ITP-01 - Information Protection Policy, Statement 1  
 UP-01 - Information Security Policy for End Users, Statement 9  
 ITS-01-03 - Access Control Standard, Baseline Requirements 1, 2, 3, 7, 8, 10, 11

#### Compliance Artifacts:

Procedures: Access Request, Access Review, Account Provisioning  
 RCD01 - Record: Access Request Tickets  
 RCD02 - Record: Access Review Log  
 RPT31 - Report: System Inventory

# Security Policies & Procedures

[Your Logo Here]

<b>Policy Title:</b>	Information Protection Policy			
<b>Policy Number:</b>	ITP-01	<b>Version:</b>	0.1	<b>Effective Date:</b> mm/dd/yyyy

Approved By: *(Authorized Signer Name)* \_\_\_\_\_ Date Approved \_\_\_\_\_

---

**Overview**

**Description**  
 This policy contains high-level information protection mandates as set forth by executive management in response to enterprise risk and regulatory compliance requirements. As with all corporate IT policies, supporting standards outline the technical security requirements and procedures outline the methods used to create or maintain security controls. The following policy statements are not meant to specify the methods of protection.

**Purpose**  
 The Information Protection Policy was set forth to protect [Company Name] from unauthorized information disclosure and other information security risks. Many of the policy statements below have been developed in response to regulatory requirements.

**Applicability**  
 There are two audiences for policies: general users and users that perform IT functions. This policy is directed at users that perform IT functions.

**Sanctions for Non-compliance**  
 This policy is compulsory. Failure to comply may result in reprimand and/or employment termination.

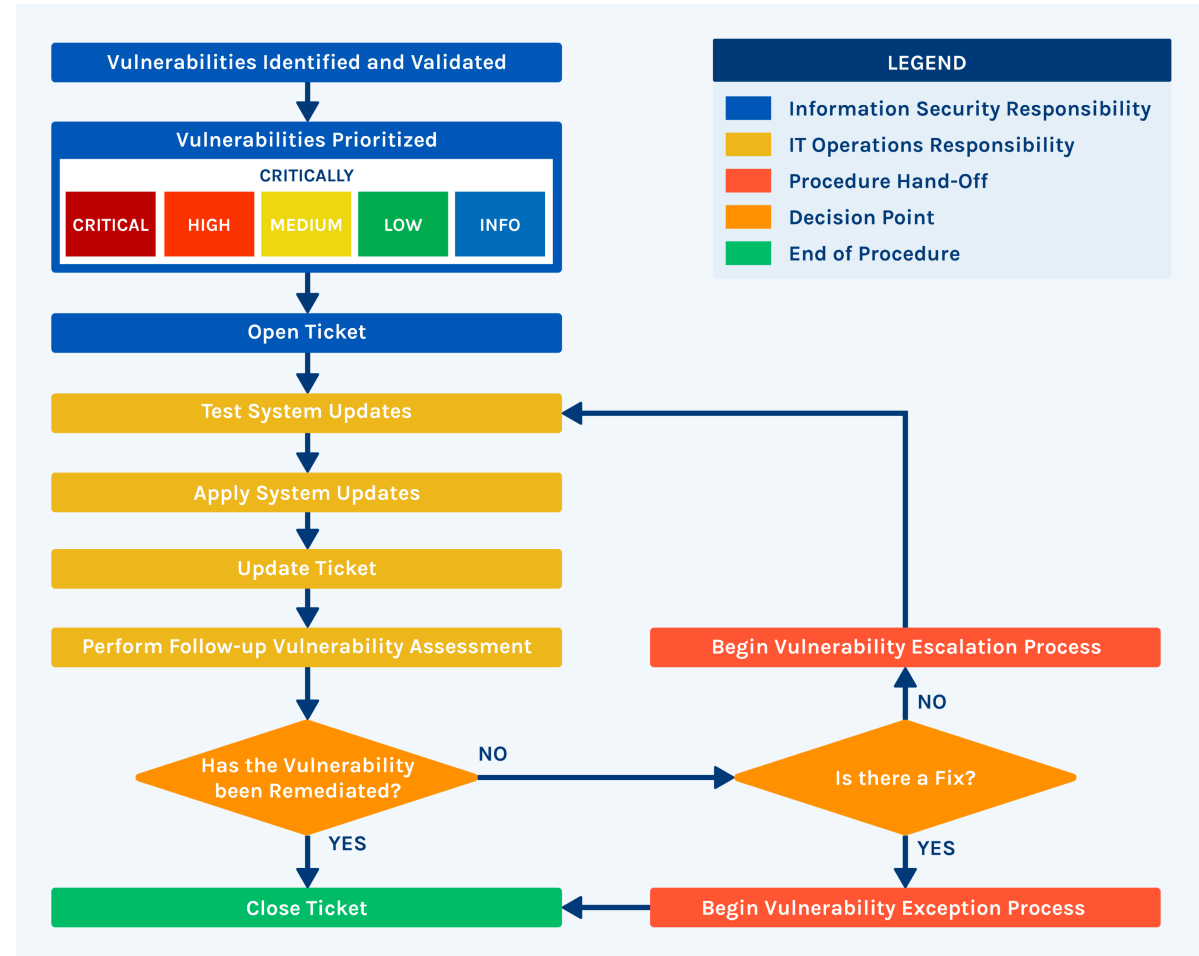
**Policy Statements**

**Policy**  
**Information will be protected in a way that reduces IT risk and complies with applicable regulations.**


**Clarifying Policy Statements**

- 1) System access must be strictly controlled. See the Access Control Standard for additional details.
- 2) Sensitive information residing on enterprise systems must be protected by appropriate security controls according to its level of sensitivity. See the Systems Security Policy and Sensitive Information Protection Standard for additional information.
- 3) Private cryptographic keys must be stored and managed in a secure manner. See the Encryption Standard for more information.
- 4) New employees, contract employees and business partners that will have access to sensitive information must undergo a background check.

Page 1 of 4 © 2013, InfoDefense, Inc., All Rights Reserved



# Governance Framework



Policy Title:	Information Protection Policy		
Policy Number:	ITP-01	Version:	0.1
Effective Date:	mm/dd/yyyy		

Approved By: *(Authorized Signer Name)* \_\_\_\_\_ Date Approved \_\_\_\_\_

**Overview**

**Description**  
This policy contains high-level information protection mandates as set forth by executive management in response to enterprise risk and regulatory compliance requirements. As with all corporate IT policies, supporting standards outline the technical security requirements and procedures outline the methods used to create or maintain security controls. The following policy statements are not meant to specify the methods of protection.

**Purpose**  
The Information Protection Policy was set forth to protect [Company Name] from unauthorized information disclosure and other information security risks. Many of the policy statements below have been developed in response to regulatory requirements.

**Applicability**  
There are two audiences for policies: general users and users that perform IT functions. This policy is directed at users that perform IT functions.

**Sanctions for Non-compliance**  
This policy is compulsory. Failure to comply may result in reprimand and/or employment termination.

**Policy Statements**

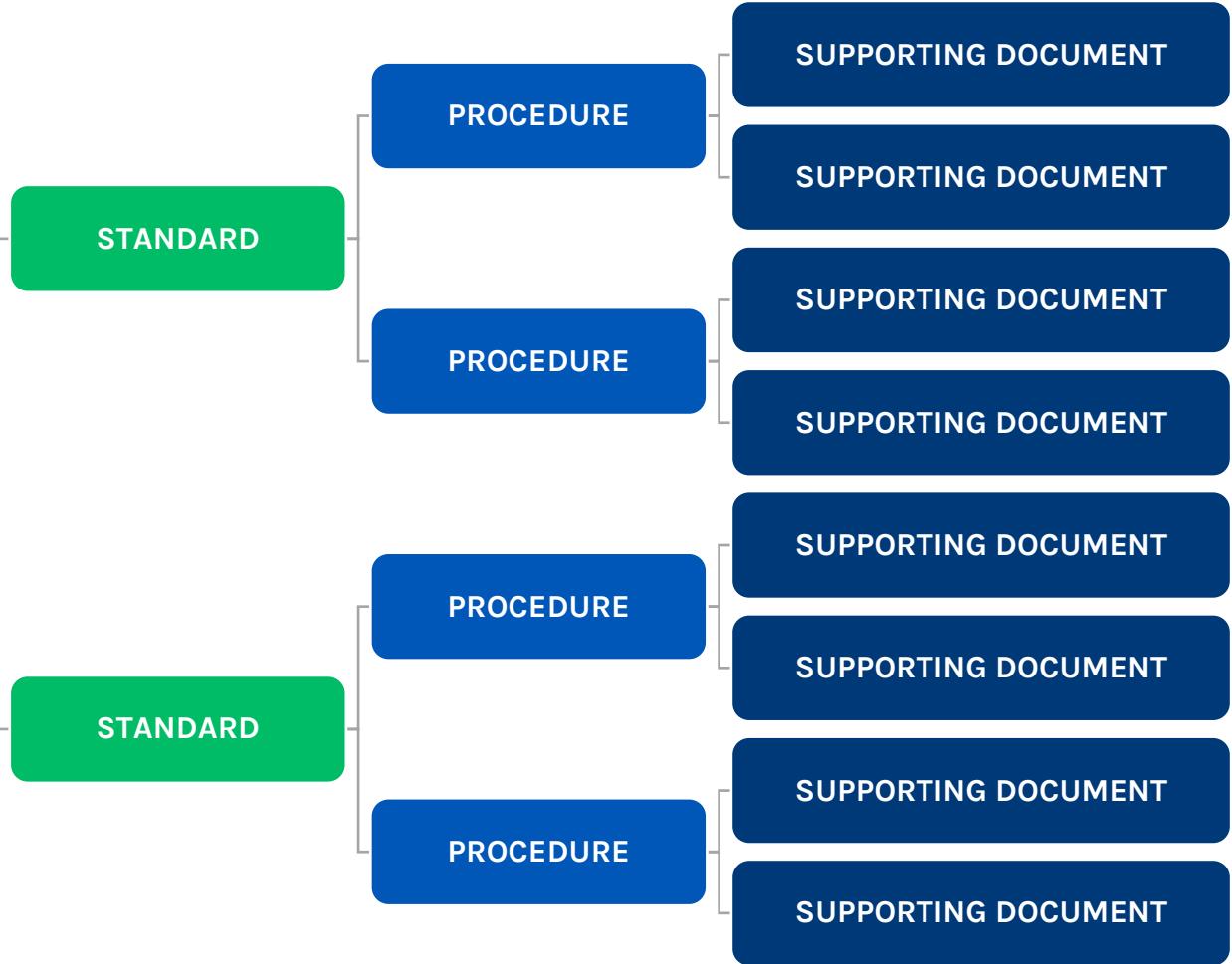
Policy  
*Information will be protected in a way that reduces IT risk and complies with applicable regulations.*

**Clarifying Policy Statements**

- 1) System access must be strictly controlled. See the Access Control Standard for additional details.
- 2) Sensitive information residing on enterprise systems must be protected by appropriate security controls according to its level of sensitivity. See the Systems Security Policy and Sensitive Information Protection Standard for additional information.
- 3) Private cryptographic keys must be stored and managed in a secure manner. See the Encryption Standard for more information.
- 4) New employees, contract employees and business partners that will have access to sensitive information must undergo a background check.

Page 1 of 4 © 2013, InfoDefense, Inc., All Rights Reserved

POLICY



# NIST CMMC Resources

An official website of the United States government [Here's how you know](#) ▾

**NIST** Information Technology Laboratory  
**COMPUTER SECURITY RESOURCE CENTER**

Search CSRC 🔍 **CSRC MENU**

**PUBLICATIONS**

## SP 800-171 Rev. 2 📄

### Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

f 🐦

**Date Published:** February 2020 (includes updates as of January 28, 2021)

**Supersedes:** [SP 800-171 Rev. 2 \(02/21/2020\)](#)

**Planning Note (4/13/2022):** 📄

The security requirements in SP 800-171 Revision 2 are available in multiple data formats. The [PDF](#) of SP 800-171 Revision 2 is the authoritative source of the CUI security requirements. If there are any discrepancies noted in the content between the [CSV](#), [XLSX](#), and the SP 800-171 [PDF](#), please contact [sec-cert@nist.gov](mailto:sec-cert@nist.gov) and refer to the PDF as the normative source.

**CUI SSP template**

\*\* There is no prescribed format or specified level of detail for system security plans. However, organizations ensure that the required information in [SP 800-171 Requirement] 3.12.4 is conveyed in those plans.

**Author(s)**  
Ron Ross (NIST), Victoria Pillitteri (NIST), Kelley Dempsey (NIST), Mark Riddle (NARA), Gary Guissanie (IDA)

**Abstract**  
The protection of Controlled Unclassified Information (CUI) resident in nonfederal systems and organizations is of

**DOCUMENTATION**

**Publication:**  
[SP 800-171 Rev. 2 \(DOI\)](#)  
[Local Download](#)

**Supplemental Material:**  
[Security Requirements Spreadsheet \(xls\)](#)  
[Security Requirements CSV \(other\)](#)  
[README for CSV \(txt\)](#)  
[CUI Plan of Action template \(word\)](#)  
[CUI SSP template \\*\\*\[see Planning Note\] \(word\)](#)  
[Mapping: Cybersecurity Framework v.1.0 to SP 800-171 Rev. 2 \(xls\)](#)

**Other Parts of this Publication:**  
[SP 800-171A](#)

**Related NIST Publications:**  
[SP 800-172](#)

**Document History:**

<https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final>



## 3. Security Monitoring & Incident Response

# Security Monitoring



# Incident Response

## Incident Response Plan

- Roles & responsibilities
- Pre-assembled toolset
- Pre-determine legal & law enforcement contacts

## Periodic incident response training exercises

- Evidence for each exercise

## 4. FIPS 140 Validated Encryption

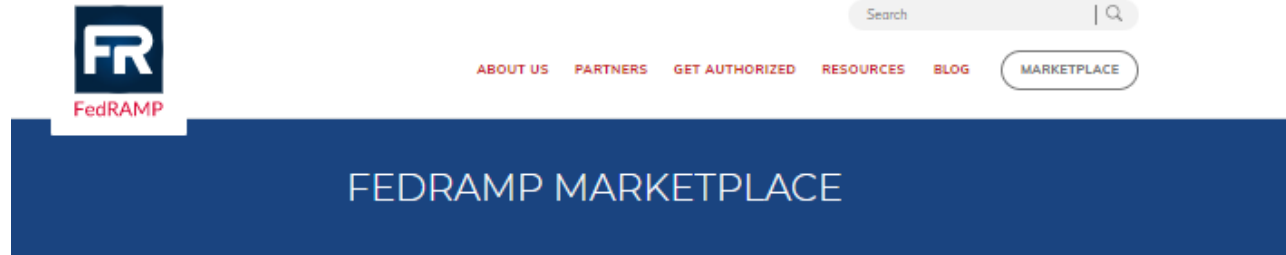
# Search FIPS-validated Modules

The screenshot shows the NIST Computer Security Resource Center (CSRC) website. At the top, there is a navigation bar with the NIST logo, the text 'Information Technology Laboratory' and 'COMPUTER SECURITY RESOURCE CENTER', and a search bar with the text 'Search CSRC' and a 'CSRC MENU' button. Below the navigation bar, there are three green buttons: 'PROJECTS', 'CRYPTOGRAPHIC MODULE VALIDATION PROGRAM', and 'VALIDATED MODULES'. The main heading is 'Cryptographic Module Validation Program CMVP', with social media icons for Facebook and Twitter. Below this is a 'Search' section with the text 'Use this form to search for information on validated cryptographic modules.' and 'Select the basic search type to search modules on the active validation list. Select the advanced search type to to search modules on the historical and revoked module lists.' The search form includes a 'Search Type:' section with radio buttons for 'Basic' (selected) and 'Advanced', and buttons for 'Search', 'Reset', and 'Show All'. Below the form are three input fields: 'Certificate Number:', 'Vendor:', and 'Module Name:'. A green banner below the form states '904 certificates match the search criteria'. At the bottom, a table header is visible with columns for 'Certificate Number', 'Vendor Name', 'Module Name', 'Module Type', and 'Validation Date'.

<https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search/all>

## 5. FedRAMP Equivalent Cloud Services

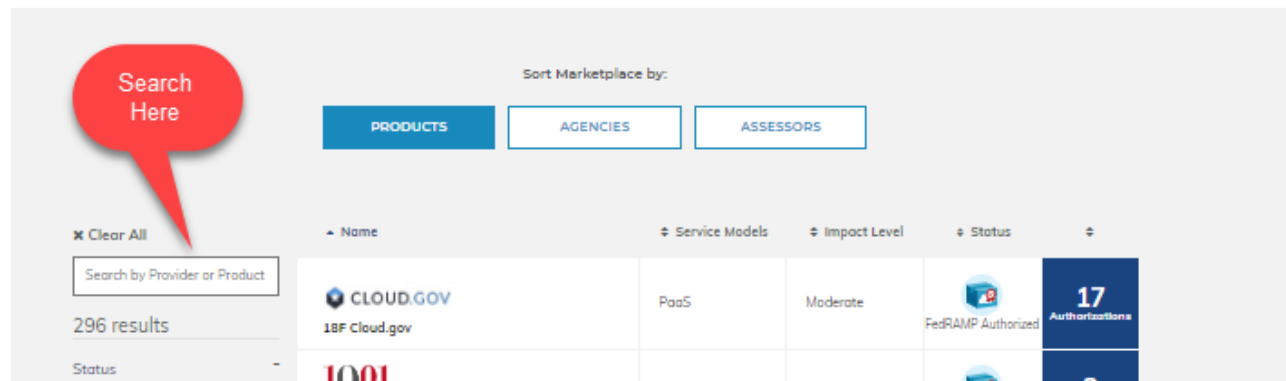
# Cloud Services



## FedRAMP at a Glance



For more information on FedRAMP designations, see [Marketplace Designations for CSPs \(PDF - 652KB\)](#).



<https://marketplace.fedramp.gov/#!/products?status=Compliant&sort=productName>

# INFODEFENSE

## Questions?



**Kevin Wheeler**

*Founder & Managing Director*

(972) 992-3100 Ext. 1101

[kevin.wheeler@infodefense.com](mailto:kevin.wheeler@infodefense.com)



# Supplemental Slides

# Web Resources

---

## **NIST SP 800-171 Rev. 2**

<https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final>

## **NIST SP 800-171A**

<https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final>

## **FIPS Validated Modules**

<https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search/all>

## **InfoDefense NIST SP 800-171 Self-Assessment Tool**

<https://www.infodefense.com/nist-sp-800-171-self-assessment-tool/>

## **DFARS 252.204-7012**

[https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting.](https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting)