INFODEFENSE

Five Steps to CMMC Compliance

Kevin Wheeler

Founder & Managing Director

Why is CMMC so Important?

Source: Katie Arrington

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
- Requirement in defense contracts as soon as 2023 (but probably in 2024)

Five Steps to CMMC Compliance

1. Assess CMMC Compliance Status
2. Develop a Plan of Action & Milestones (POA&M)
3. Create a System Security Plan (SSP)
4. Implement Security Capabilities
5. Gather Evidence to Demonstrate Compliance

CMMC Preparation Effort

CMMC Preparation Task	Time	Expertise
Gap Analysis	2 Weeks+	High
Plan of Action & Milestones	2 Months+	Medium
System Security Plan	4 Months+	High
Remediation	**12 Months+***	**High**
Evidence Collection	3 Months	Low

* Assuming Low NIST SP 800-171 Compliance Level

1. Assess CMMC Compliance Status

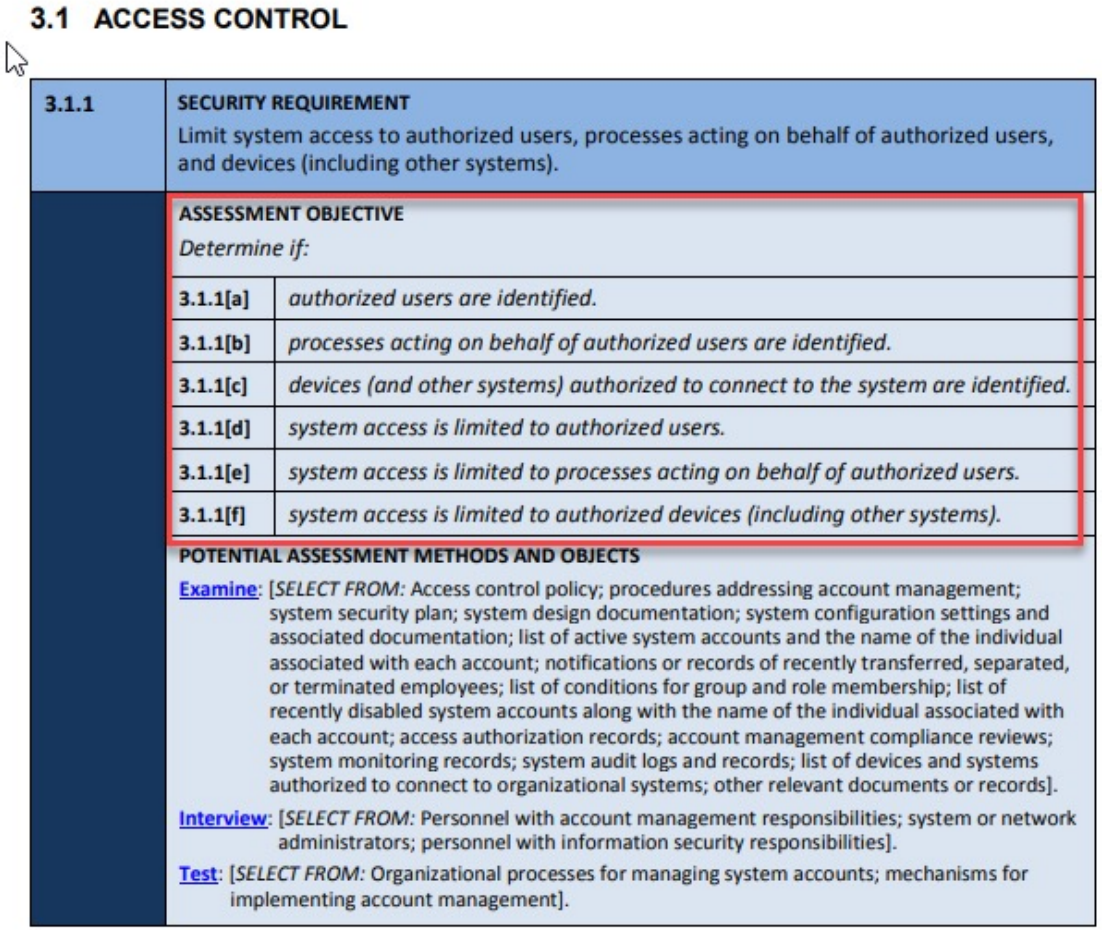
NIST SP 800-171 Gap Analysis

INFODEFENSE		compliance-help@infodefense.com | (972) 992-3100			
CMMC Ref.	Requirement	Status	Justification	Defiency	Remidiation
ACCESS CONTROL					
Security Requirements					
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	Not Compliant	Notes from the assessment	No clear process for adding, disabling, and deleting an account. No Policies, Standards or procedures. No clear ownership of who can add, disable and delete accounts. Passwords are similar & shared.	Implement policies, standards and procedures that define roles and responsibilities for access control. Create unique ID's for each person and or service that require access for information systems. Implement a clear process for account changes, and who is authorized to request them. Ensure that audit logs are configured to ensure clear ownership of account changes.
AC.1.002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	Not Compliant	Notes from the assessment	No Policies, Standards or procedures. No formal process for account management standard.	Implement policies, standards and procedures for access control and account management. Implement procedures to enforce standards and make them actionable. Implement with Group Policy restrictions to what a user can access based on their department and account.
AC.1.003	Verify and control/limit connections to and use of external information systems.	Not Compliant	Notes from the assessment	No Policies, Standards or procedures. No DNS Filtering.	Implement policies, standards and procedures to enforce verification and control of connections to external systems. Implement web content and DNS filtering at the Internet gateway firewall. Perform firewall reviews.
AC.1.004	Control information posted or processed on publicly accessible information systems.	Not Compliant	Notes from the assessment	No Policies, Standards or procedures. No security awareness training.	Implement policies, standards and procedures to address the posting of company information, specifically CUI. Implement security awareness training to ensure that end users are aware of the threats of posting sensitve information such as CUI to social media platforms.
AC.2.005	Provide privacy and security notices consistent with		Notes from the assessment	No Policies, Standards or procedures.	Implement policies, standards and procedures to provide privacy

InfoDefense CMMC/NIST SP 800-171 Self-Assessment Tool

NIST SP 800-171 Assessment Objectives

- Download NIST SP 800-171A
- Review Assessment Objectives for Each Security Requirement
- Don't Overlook NFO Controls in NST SP 800-171, Rev 2 – Appendix E



3.1 ACCESS CONTROL

3.1.1	**SECURITY REQUIREMENT** Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).

ASSESSMENT OBJECTIVE

Determine if:

3.1.1[a]	*authorized users are identified.*
3.1.1[b]	*processes acting on behalf of authorized users are identified.*
3.1.1[c]	*devices (and other systems) authorized to connect to the system are identified.*
3.1.1[d]	*system access is limited to authorized users.*
3.1.1[e]	*system access is limited to processes acting on behalf of authorized users.*
3.1.1[f]	*system access is limited to authorized devices (including other systems).*

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine: [*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].

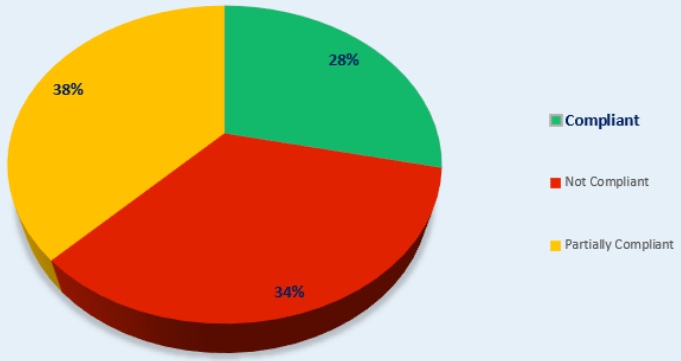
Interview: [*SELECT FROM:* Personnel with account management responsibilities; system or network administrators; personnel with information security responsibilities].

Test: [*SELECT FROM:* Organizational processes for managing system accounts; mechanisms for implementing account management].

Submit Your SPRS Score

CMMC Level 2 Status

28% Compliant SPRS Score -127 / 110



Percentage Compliant

28%

SPRS Assessment Scoring (NIST 800-171)

NIST SP 800-171 DoD Assessment Scoring Methodology (As Defined by DoD)

The NIST SP 800-171 DoD Assessment will result in a score reflecting the net effect of security requirements not yet implemented. If all security requirements are implemented, a contractor is awarded a score of 110, consistent with the total number of NIST SP 800-171 security requirements. For each security requirement not met, the associated value is subtracted from 110. The score of 110 is reduced by each requirement not implemented, which may result in a negative score.

Current Score	Total
-127	110

Common Reasons for Inaccuracies

- Inadequate polices, standards and other compliance-related documentation
- Security monitoring and incident response capabilities
- “FIPS Compliant” vs. “FIPS Validated” Encryption (FIPS Validated Modules)
- FedRAMP Equivalency Required for Cloud Services

2. Develop a POA&M

Plan of Action & Milestones

- Remediation plan in DoD recognized format
- Include all CMMC compliance gaps identified in Step 1
- NIST publishes a template on NIST SP 800-171A web page.

POA&M ID	NIST Ref.	Weakness	Responsible Team	Security Controls	Point of Contact	Human Resources Required	Processes & Technology Required	Completion Date	Milestones with Completion Dates	Changes to Milestones	Deficiency Identified by	Risk Level (Low/Med/High)	Estimated Cost	Status	Comments
1	3.1.1 3.1.2 3.13.3	There is no written procedure that covers access chages.	IT Operations	Develop a process to manage changes to user access for instances such as changes in job roles and terminations.	Jonathan Archer	1 FTE	Policy, Standards & Procedures	30-Aug-23	Create an account request authorization procedure. Utilize least privilege for all users.		James Kirk	Med		On Hold	
2	3.1.3	There is no policy that governs the flow of CUI in the organization.	IT Operations	Develop a policy to govern the flow of CUI so that only users that have a bonafide business requirement for CUI access are permitted access to CUI.	Benjamin Sisco	1FTE	Policy, Standards & Procedures	30-Aug-23	Develop CUI Governance Posticy Limit access to CUI that is in physical format. Limit access to CUI that is in logical format.		Jame Kirk	Med		Not Started	
												Select...		Select...	
												Select...		Select...	
												Select...		Select...	
												Select...		Select...	

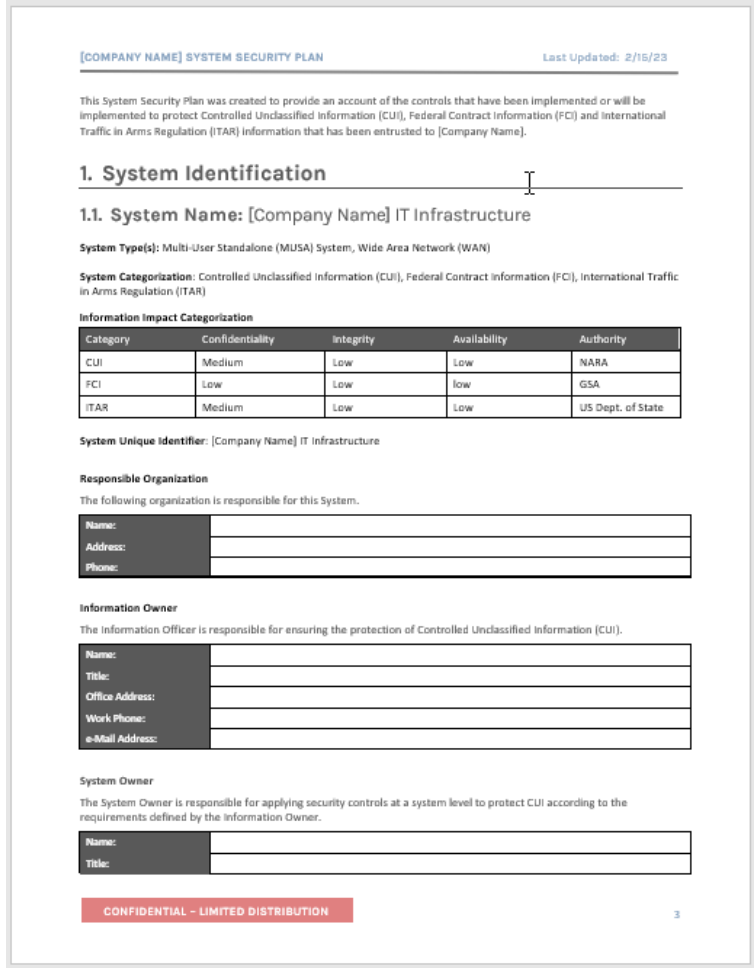
NIST CMMC Resources

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

3. Create a System Security Plan (SSP)

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: 2/15/23

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 website

4. Implement Security Capabilities

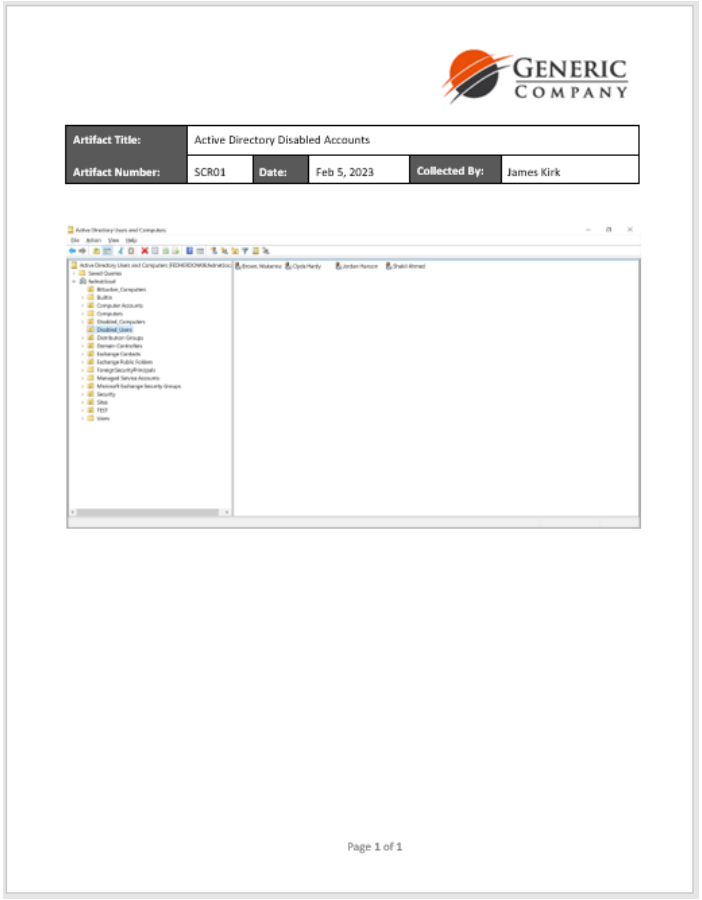
Cyber Security Program Elements

- ✓ Plan of Action & Milestones
- ✓ System Security Plan
- ✓ Detailed security, network, and system diagrams
- ✓ Information Flow Analysis for CUI and FCI
- ❑ Policies, standards and procedures that address all practices
- ❑ Centralized security logging and alerting
- ❑ Continuous security and compliance monitoring
- ❑ Standard secure server and workstation configurations
- ❑ Vulnerability management program
- ❑ Strong logical access control (including multi-factor authentication)
- ❑ Periodic risk & security assessment
- ❑ Security awareness program
- ❑ Mobile device management
- ❑ Cyber incident response capability (plan, training, tools)
- ❑ FIPS validated encryption
- ❑ Firewall, malware protection, DNS filtering, web content filtering, etc.

5. Gather CMMC Compliance Evidence

Artifacts

- **Gather** screenshots. pictures, records, reports, logs and other evidence
- **Organize** artifacts in a referenceable format
- **Reference** artifacts from the System Security Plan

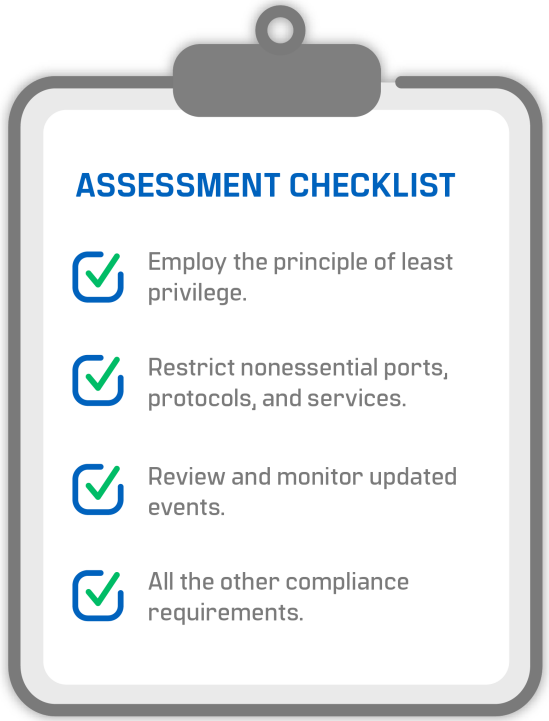

GENERIC COMPANY

Artifact Title:	Active Directory Disabled Accounts				
Artifact Number:	SCR01	Date:	Feb 5, 2023	Collected By:	James Kirk

Page 1 of 1

CMMC Certification Process

- Assessed by third-party assessor organization (C3PAO)
- Certification will last 3 years
- Requires a comprehensive cyber security program



CMMC Benefits

- Stay ahead of DoD requirements
- Increase cyber security posture
- Demonstrates cyber security is taken seriously
- Competitive Advantage

Next Steps

- Complete your Gap Analysis
- Submit your SPRS Score
- Create your POA&M and SSP
- Begin work toward full compliance

INFODEFENSE

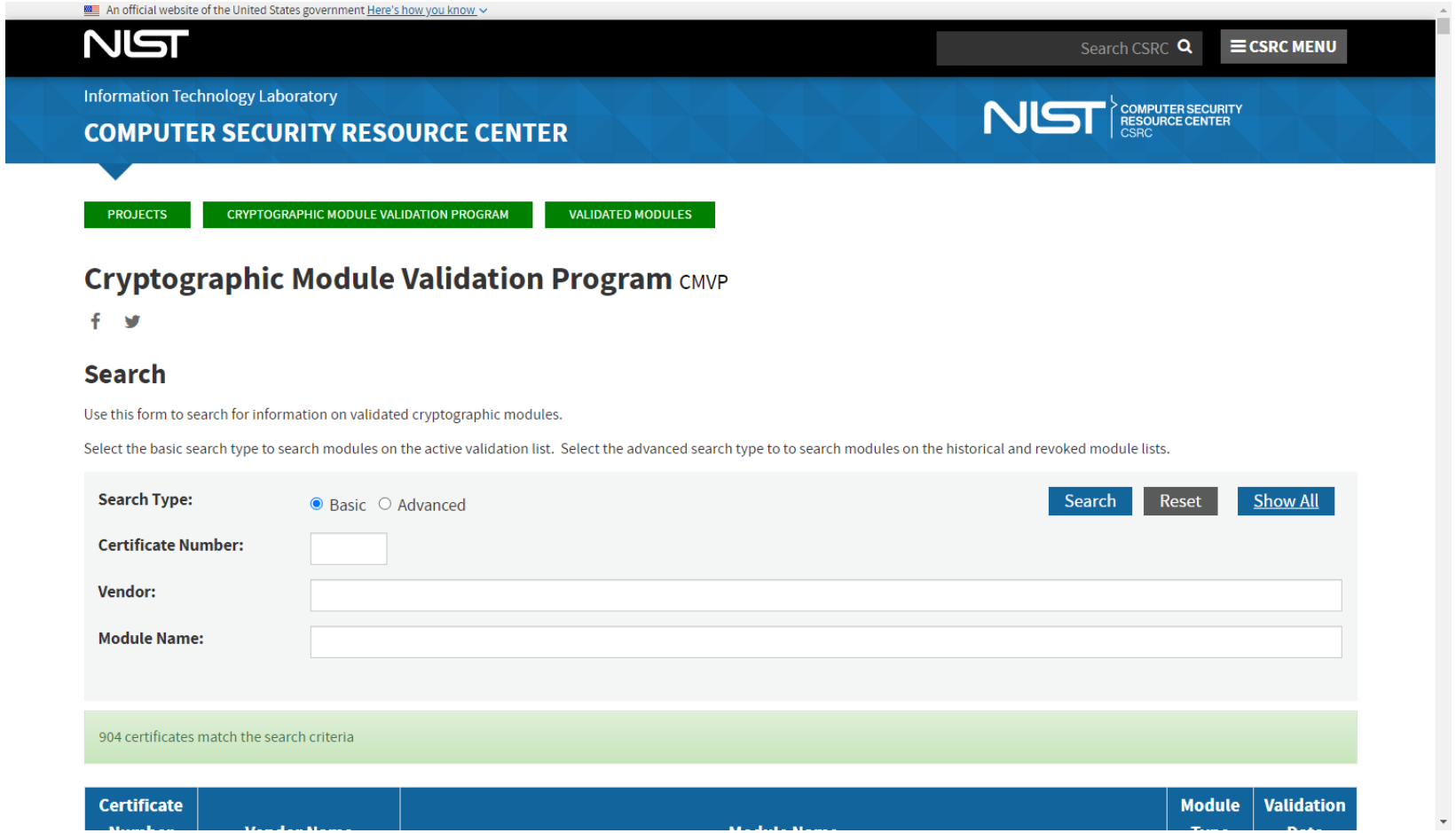
Questions?

- Meet with an InfoDefense CMMC Compliance Expert
- View InfoDefense Webinar Transcript and Q&A

Kevin Wheeler
Founder & Managing Director
(972) 992-3100 Ext. 1101
kevin.wheeler@infodefense.com

Supplemental Slides

Search FIPS-validated Modules



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

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.