



PROJECT SPECTRUM

Defending Your Business in Cyberspace

Presenter: Kareem A. Sykes, Director of Industry & Engagement

Audience: Small Business Bootcamp Conference 2026

Date: March 25, 2026



MEET THE PRESENTER



Mr. Kareem A. Sykes

Project Spectrum
Industry & Engagement, Director
Eccalon, LLC

Project Spectrum is a Department of War (DoW) recognized cybersecurity awareness initiative that provides the tools and training to increase cybersecurity awareness and maintain compliance with DoW contracting requirements.

TODAY'S AGENDA

Project Spectrum's Mission: Educate businesses on the landscape of cybersecurity

- About Project Spectrum
- Current Cyber Threat Landscape
- Federal Contract Information (FCI) and Controlled Unclassified Information (CUI)
- Foreign Ownership, Control, or Influence (FOCI)

Overview of federal regulations for safeguarding data and information

- Title 48 CFR (CMMC) Final Rule Published in Federal Register
- Cybersecurity Maturity Model Certification (CMMC) Program
 - CMMC Level 1
 - CMMC Level 2
 - CMMC Level 3
 - Assessment Requirements
- Compliance Scenario

How Project Spectrum can assist

- Project Spectrum Resources
- ProjectSpectrum.io Website Update

ABOUT PROJECT SPECTRUM

Project Spectrum Bolsters Homeland Defense

The DoW Office of Small Business Programs initiated Project Spectrum as a comprehensive platform to provide the tools and training needed to increase cybersecurity awareness and maintain compliance in accordance with DoW contracting requirements.

Project Spectrum Advances National Security Priorities

- Strengthens national security by supporting businesses that provide technological solutions to reestablish deterrence and modernize the defense industrial base.
- Supports homeland defense and our warfighters by providing businesses with the most up-to-date cybersecurity compliance education, tools and training.

Citation Authorities:

10 U.S.C. § 2224 note

15 U.S.C. § 638 note

10 U.S.C. § 4901 note



IT'S OFFICIAL CMMC HAS ARRIVED!!!

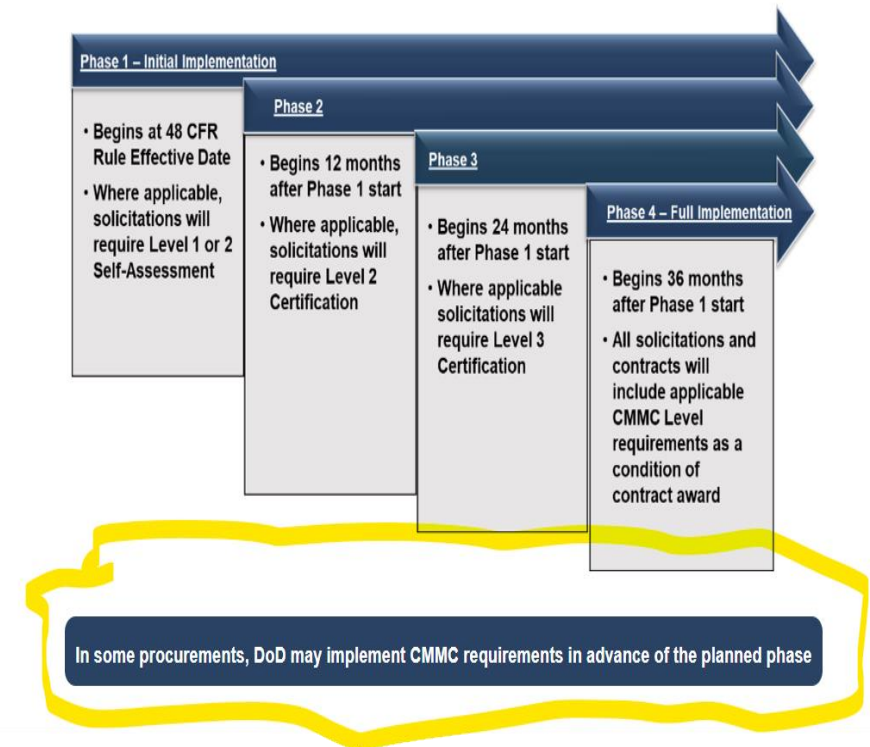
The 48 CFR CMMC final rule was officially published on 9/10/2025.

- The rule went into effect on 11/10/2025.
- This triggered the first of the 4 phase of CMMC 'Phased Rollout'.
- Virtually all new DoW solicitations will include some level of CMMC requirement.

Note: CMMC Level 2 certification assessments can and will be required during Phase 1.

CMMC Implementation

The CMMC Program implementation date is 60 days after the publication of the final Title 48 CFR CMMC acquisition rule. CMMC assessment requirements will be implemented using a four-phase plan over three years. The phases add CMMC Level requirements incrementally, starting with self-assessments in Phase 1 and ending with full implementation of program requirements in Phase 4. This phased approach allows time to train assessors and for companies to understand and implement CMMC assessment requirements.



<https://DoWcio.defense.gov/cmmc/About/>

WHY IT ALL MATTERS

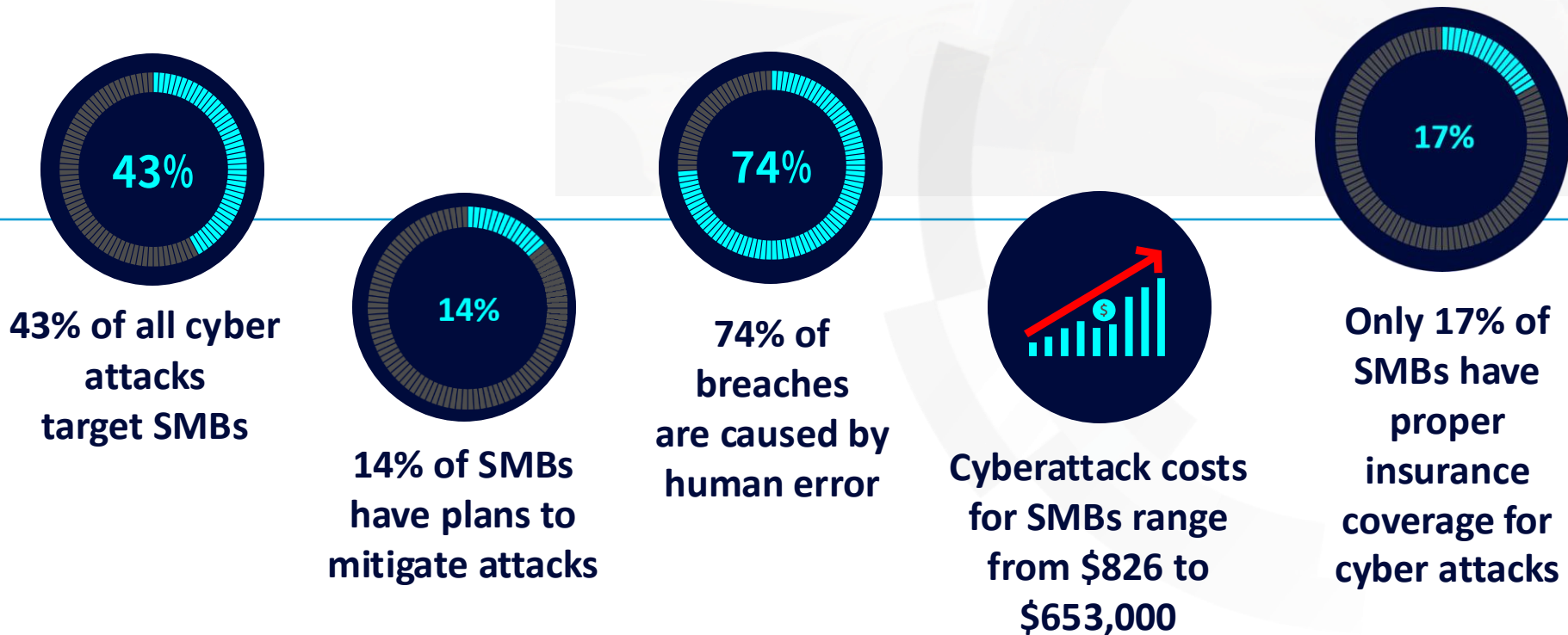
OVERVIEW OF THE CYBER THREAT LANDSCAPE & FEDERAL REGULATIONS



EDUCATION: THREAT LANDSCAPE

The Defense Industrial Base (DIB) is Under Attack:

Small & Medium Businesses (SMBs) are on the Front Line



Why are SMBs targeted?

- Intellectual property and trade secrets
- Dual-use technologies
- Access to sensitive government information
- Interconnection with larger defense contractors, supply chain
- Political / ideological motivation

Federal Contract Information (FCI)

FAR Clause “52.204-21”

FCI is sensitive, but not classified, information that is provided by or generated for the government under a contract. FCI refers to information not intended for public release.

Controlled Unclassified Information (CUI)

DFARS Clause “252.204-7012”

While unclassified, CUI is information that the U.S. federal government creates or possesses, or that an entity creates or possesses for or on behalf of the government, and that a law, regulation, or government-wide policy requires or permits an agency to protect via safeguarding or dissemination controls.



FCI Examples

- Contract information
- Organizational charts
- Process documentation
- Contract performance reports
- RFP or RFI responses

CUI Examples

- Proprietary Business Information (PBI)
- Unclassified Controlled Technical Information (UCTI)
- Sensitive but Unclassified (SBU)
- For Official Use Only (FOUO)
- Law Enforcement Sensitive (LES)

FOREIGN OWNERSHIP, CONTROL, OR INFLUENCE

- Foreign Ownership, Control or Influence (FOCI) happens when a foreign entity has the power to direct or influence the management or operations of a company. This can lead to unauthorized access to sensitive information and potentially compromise national security.
- FOCI issues affect a company's ability to qualify for and maintain eligibility to contract with the government.
- The **manufacturing sector accounts for more than 22% of reported cyber espionage incidents**, and FOCI is one of the major risk vectors.
- **FY 2023 NDAA Section 875** requires DoW to establish a program that demonstrates “commercial due diligence tools, techniques, and processes” to help small businesses identify “attempts by malicious foreign actors to gain undue access to, or foreign ownership, control, or influence over the business.”



After you register for Project Spectrum, you will have access to our FOCI training course which covers:

- Properly identifying FOCI
- Evaluating the impact of FOCI
- Reducing FOCI risks

Cybersecurity Maturity Model Certification (CMMC)



CMMC MODEL

- CMMC Level 1 is considered “**Foundational**” for basic data safeguarding for businesses that only handle FCI data.
- CMMC Level 2 is considered as “**Advanced**” for enhancing data safeguarding for businesses that handle “Basic” and “Specified” CUI data acquisitions.
- CMMC Level 3 is considered as “**Expert**” for high capacity in safeguarding **CUI data related to national security programs or high-value assets** and includes an additional 24 requirements.

CMMC Model	Model	Assessment
LEVEL 3	134 requirements (110 from NIST SP 800-171 r2 plus 24 from 800-172)	<ul style="list-style-type: none">• DIBCAC assessment every 3 years• Annual Affirmation
LEVEL 2	110 requirements aligned with NIST SP 800-171 r2	<ul style="list-style-type: none">• C3PAO assessment every 3 years, or• Self-assessment every 3 years for select programs.• Annual Affirmation
LEVEL 1	15 requirements aligned with FAR 52.204-21	<ul style="list-style-type: none">• Annual self-assessment• Annual Affirmation



ASSESSMENT REQUIREMENTS: CMMC LEVEL 1

- **Annual self-assessments** for all DIB contractors that handle FCI data are required.
- To be compliant, all findings must result in a **“Met”** or **“N/A”** status. **Note:** Plans of Action & Milestones (POAMs) are not permitted at Level 1.
- Self-assessments results must be submitted to the **Supplier Performance Risk System (SPRS)**.
- When conducting self-assessments, a CMMC certification is **NOT required or issued** at this level.
- Organizations can register with **Project Spectrum at no-cost** to conduct assessments and produce scores.



ASSESSMENT REQUIREMENTS: CMMC LEVEL 2

CMMC Level 2 is bifurcated based on DIB contractors that handle CUI data acquisitions. There are two compliance tracks. Each requiring a minimum passing score of 88 out of 110

Self Attestation

- **Annual self-assessments**
- Businesses can create **financial savings** by using Project Spectrum's assessment tools, training, and cyber advisory preparedness services.
- CMMC certification is NOT required or issued.
- Scores are uploaded to the **Supplier Performance Risk System (SPRS)**.

Certification

- **A triennial (every 3-year cycle) assessment**
- Certification must be performed by CMMC Certified Third-Party Assessment Organizations (C3PAOs).
- Businesses can create **financial savings** by using Project Spectrum's assessment tools, training, and cyber advisory preparedness services.
- Assessments must be submitted to the **CMMC Enterprise Mission Assurance Support Services (EMASS) system**.

ASSESSMENT REQUIREMENTS: CMMC LEVEL 2

Check the National Archives Records Administration (NARA) Organizational Index Groupings
<https://www.archives.gov/cui/registry/category-list>

If the CUI data that your company handles, falls into the following category data types, your company will need to be assessed by a CMMC Third Party Assessment Organization (C3PAO) to achieve CMMC Level 2 Certification.

Defense:

- Controlled Technical Information
- DoW Critical Infrastructure Security Information
- Naval Nuclear Propulsion Information
- Privileged Safety Information
- Unclassified Controlled Nuclear Information - Defense

ASSESSMENT REQUIREMENTS: CMMC LEVEL 3

- A triennial (every 3-year cycle) assessment and certification renewal is required.
- All CMMC Level 3 requirements are valued at 1 point each. Max score of 24 points.
- **Pre-Requirement:** Must have achieved CMMC Level 2 status.
- Requires annual affirmation.
- Assessment to be conducted via Defense Contract Management Agency “DCMA – DIBCAC.”
- Assessments must be submitted to the **CMMC Enterprise Mission Assurance Support Services (EMASS)** system.



CMMC Compliance Journey

Process overview for meeting CMMC compliance requirements utilizing Project Spectrum



Compliance Scenario – CMMC Compliance Journey



STEP 1 – Select the Appropriate CMMC Level

To determine the appropriate CMMC level, businesses must determine the type of data they are managing for their contract.

- The federal entity requesting services from a business shall determine FCI or CUI requirements in the request for quote (RFQ), request for proposal (RFP), and or supporting contract documentation.
- Businesses should consult with their Contracting Officer for clauses in existing contracts.



Federal Contract Information (FCI) Data

Data generated for the Federal Government under a contract to develop or deliver a product or service and is not intended for public release.

Controlled Unclassified Information (CUI) Data

Information that requires safeguarding and may also be subject to dissemination controls. See DoW CUI Registry by visiting <https://www.DoWcui.mil/CUI-Registry-New/>

STEP 2 – Conduct a CMMC Self-Assessment Scope

Within the Project Spectrum platform, CMMC Scoping Assessment tools can be used to inform which assets within the contractor's environment will be assessed and the details of the self-assessment.

The screenshot shows the Project Spectrum (PS) platform interface for a CMMC Level 1 Self-Assessment. The header includes the PS logo and navigation links: Cyber Corner, Courses/Videos, Events, Info Hub, Useful Tools, and My Account. The main heading is "CMMC Level 1 Self Assessment" with a sub-heading "Introduction to Level 1 Self-Assessment".

The content area is titled "Access Control (AC) AC.1-8.1- AUTHORIZED ACCESS CONTROL" and "AC.1-8.1- AUTHORIZED ACCESS CONTROL (Federal Contract Information (FCI) DATA)". It provides a description: "Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems)."

It includes sections for:

- Technical Explanation:** Use tools like Active Directory to enforce access control policies, ensuring only authorized users and devices can connect to your systems. Employ account management processes to restrict access based on roles.
- Non-Technical Explanation:** Only allow trusted employees and devices to access your systems. Ensure everyone has unique login credentials.
- Required Documents:**
 - o Access control policy
 - o System configuration settings
 - o List of authorized users and devices
- Example:** Maintain a list of employees with access to company computers. Use software to ensure only these users can log in to your network.

The assessment question is: "1. AC.1-8.1- AUTHORIZED ACCESS CONTROL (FCI DATA) *
Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems)."

Two questions are visible with radio button options:

- Authorized users are identified? Yes No Not Applicable Answer Later
- Processes acting on behalf of authorized users are identified? Yes No Not Applicable Answer Later

A yellow question mark icon is visible in the bottom right corner of the assessment area.

Scoping for CMMC Level 1

[CMMC Level 1 Scoping Documentation](#)

- Focus on FCI assets
- Covers 6 family domains

Scoping for CMMC Level 2

[CMMC Level 2 Scoping Documentation](#)

- Focus on CUI assets
- Covers 14 family domains
- Must produce System Security Plans (SSP) and Plan of Actions & Milestones (POA&M) documentation

STEP 3 – Conduct a CMMC Self-Assessment

The Project Spectrum Self-Assessment tools are used to examine how a company is safeguarding data. The self-assessment documentation provides companies with the overall process, how to document compliance, criteria, methodology, and practice findings.

- No-cost assessment, saving companies money
- Adheres to FAR Clause 52.204-21 and NIST 800-171A
- Assessment objects are examined and tested
- Documentation created/updated for evidence
- *To be compliant, the contractor needs all findings to result in a “Met” or “N/A” status*
- Can inherit practice objectives from an External Service Provider (ESP)

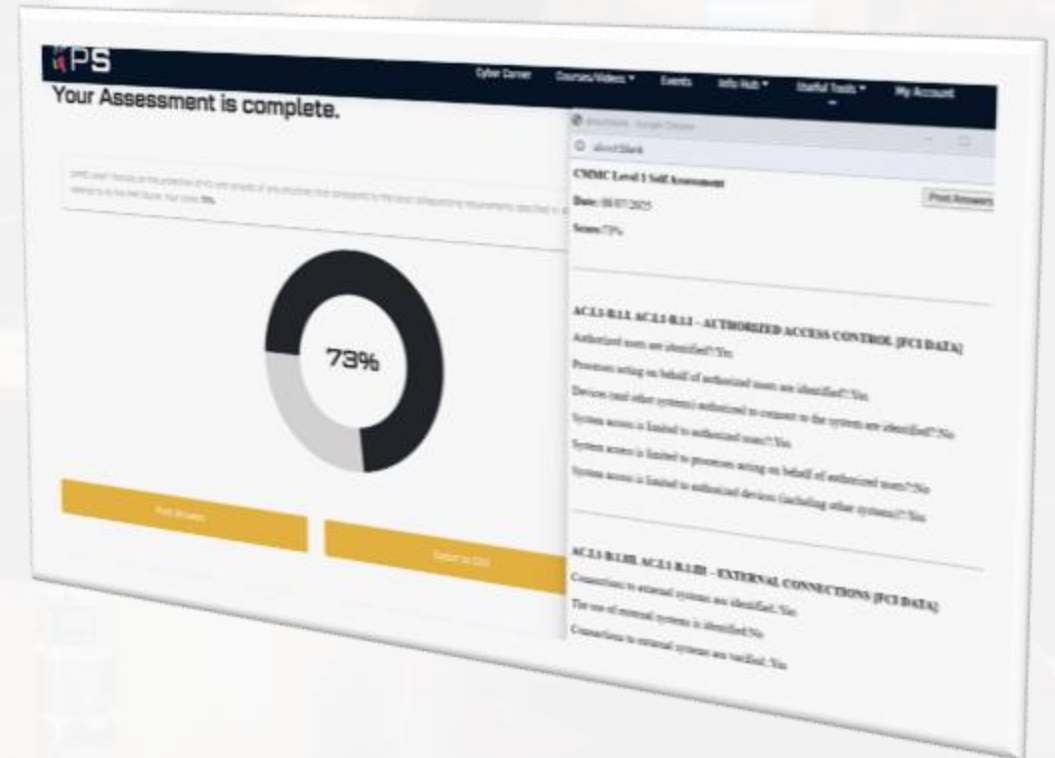
[CMMC Self-Assessment Guide \(Level 1\)](#)

The screenshot shows the 'CMMC Level 1 Self-Assessment' tool interface. The header includes the 'PS' logo and navigation links: 'Cyber Corner', 'Courses/Videos', 'Events', 'Info Hub', 'Useful Tools', and 'My Account'. The main content area is titled 'CMMC Level 1 Self-Assessment' and 'Introduction to Level 1 Self-Assessment'. It details the 'Access Control (AC) AC.L1-B.1.1 - AUTHORIZED ACCESS CONTROL' requirement, specifically 'AC.L1-B.1.1 - AUTHORIZED ACCESS CONTROL [Federal Contract Information (FCI) DATA]'. The requirement text states: 'Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems)'. It includes sections for 'Technical Explanation', 'Non-Technical Explanation', 'Required Documents', and 'Example'. The 'Required Documents' list includes: 'Access control policy', 'System configuration settings', and 'List of authorized users and devices'. The 'Example' states: 'Maintain a list of employees with access to company computers. Use software to ensure only these users can log in to your network.' Below this, a question is presented: '1. AC.L1-B.1.1 - AUTHORIZED ACCESS CONTROL [FCI DATA] * Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). Authorized users are identified?' with radio button options for 'Yes', 'No', 'Not Applicable', and 'Answer Later'. Similar questions and options are visible for 'Processes acting on behalf of authorized users are identified?' and 'Devices (and other systems) authorized to connect to the system are identified?'. A question mark icon is visible in the bottom right corner of the interface.

STEP 4 – Perform a Gap Analysis

Once the self-assessment is conducted, businesses should conduct a gap analysis to assess their organization's current cybersecurity posture against the specific CMMC requirements.

- Project Spectrum produces a findings report
- A scoring methodology is used to produce an assessment score
- Businesses use the findings report to begin their gap analysis by identifying control results
- Identify control gaps and identify those that report a **“Not Met”** or **“No”** status
- Review Project Spectrum’s Micro Lessons
- Align gaps with CMMC Level requirements



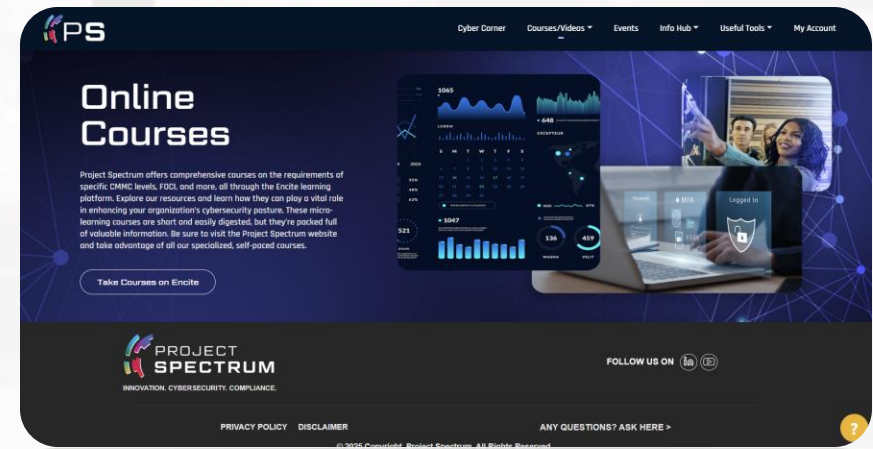
STEP 5 – Develop a Remediation Plan

A remediation plan is developed to address and rectify identified security gaps, deficiencies, or vulnerabilities within an organization's cybersecurity controls. It outlines the specific actions, resources, timelines, and steps necessary to close these gaps and enhance security.



- Identify and prioritize gaps
- Conduct a risk assessment
- Set clear objectives and action items
- Determine the resources
- Establish realistic timelines
- Document all remediation efforts
- Test and validate
- Determine continuous improvement

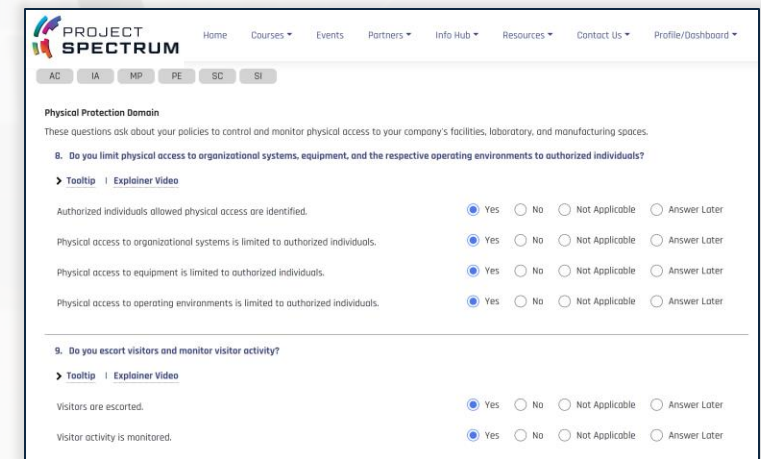
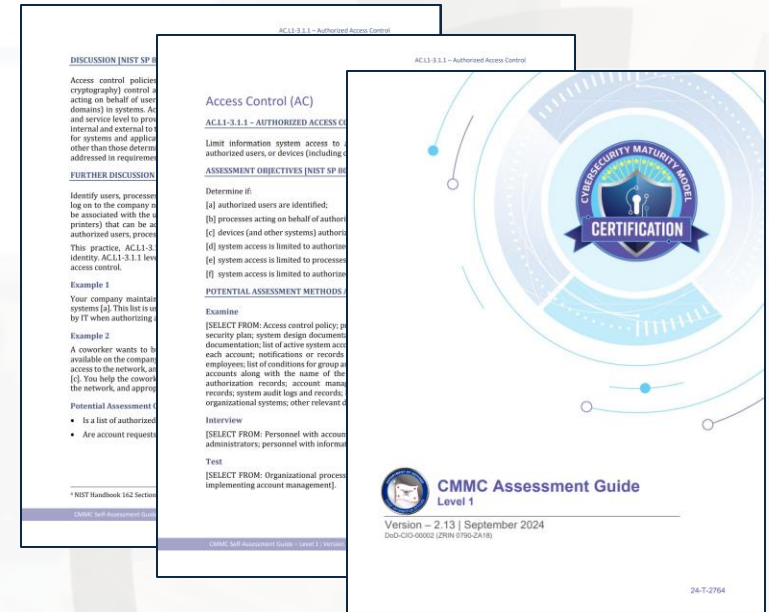
Project Spectrum Micro Lessons Learn how and what to implement



STEP 6 – Implement Security Controls

The implementation process is a critical step towards remediating the gaps that were found after conducting the self assessment process. Consider the following steps for the remediation plan and implementation process:

- Businesses use CMMC Assessment Guides with the Project Spectrum Self-Assessment tool to implement controls
- Planning and preparation
- Learning and applying the DoW Risk Assessment
- Selecting the GAP Security Controls
- Implementing, remediating each GAP Security Control
- Collecting Evidence
- Updating documentation: plans, policies, processes and procedures
- Continuous monitoring on current posture



STEP 7 – Prepare Documentation and Evidence

Proper documentation serves as evidence that an organization has implemented and is following the required security controls. All documents need to be in their final form. Examples of documents that can be used as part of the documentation evidence are:

- Policies, processes, and procedures documents
- Plans and planning documents
- System, network, and data flow diagrams
- System, network, and data configurations
- Training materials



CYBER ADVISORY SERVICES

If the business is struggling with identifying their policies, processes, plans, security controls, documentation, and other compliance requirements, Project Spectrum Cyber Advisors are here to assist.



support@projectspectrum.io

COMPLIANCE SCENARIO

STEP 8 – Conduct Assessment

DoW requires contractors to conduct a “basic” assessment and produce an assessment score to be uploaded to the Supplier Performance Risk System (SPRS), DoW's authoritative source for supplier and product performance information.

SPRS Website: [Supplier Performance Risk System](#)

- Procurement Integrated Enterprise Environment (PIEE) access is required
- SPRS application access is required
- The score obtained from the Project Spectrum self-assessment tool will be used to upload to SPRS
- Contracting Officers and their representatives shall verify a company's assessment score in SPRS

NIST SP 800-171 ASSESSMENT

Assessment Date:

Score:

Assessing Scope: -Select-

Plan of Action Completion Date:

System Security Plan (SSP) Assessed:

SSP Version/Revision:

SSP Date:

Included CAGE(s): [Open CAGE Hierarchy](#)

Include HLO

How to Enter Your Project Spectrum NIST SP 800-171 Score into SPRS

Learn how to enter and edit an assessment in your SPRS account.

Detail View:
A3 COMPANY - [\(Return to Top\)](#)

[+](#) Add New Assessment [Y](#) Clear All Filters [C](#) Refresh

	DFARS 252.204-7012 Compliance	Most Recent Assessment	Assessment Score	Confidence Level	Standard used to Assess	Assessing CAGE or DoDAAC	Assessment Scope	Included CAGE/entities	Plan of Action Completion Date	System Security Plan Assessed	System Security Plan Version/Revision	System Security Plan Date
		06/16/2021	110	BASIC	NIST SP 800-171		ENTERPRISE	IAAA3 A3 COMPANY	06/16/2021	Company A3 SSP		06/16/2021
		05/11/2021	110	BASIC	NIST SP 800-171		ENCLAVE	IAAA4 A4 COMPANY	N/A	2021-469	1	05/10/2021

1 - 2 of 2 items

PROJECT SPECTRUM'S CYBERSECURITY RESOURCE PROVISIONING





Katie Arrington

Former Performing the Duties of the Department of War Chief Information Officer, in an interview with GovCIO Media & Research

“I see CMMC being enduring. What we’re hoping to do, as it goes into effect this year, is figure out how to evolve it and make it more dynamic. It’s going to have problems. There are going to be issues when it rolls out. I always say, I like to fail early and fail often to get to what I need.”





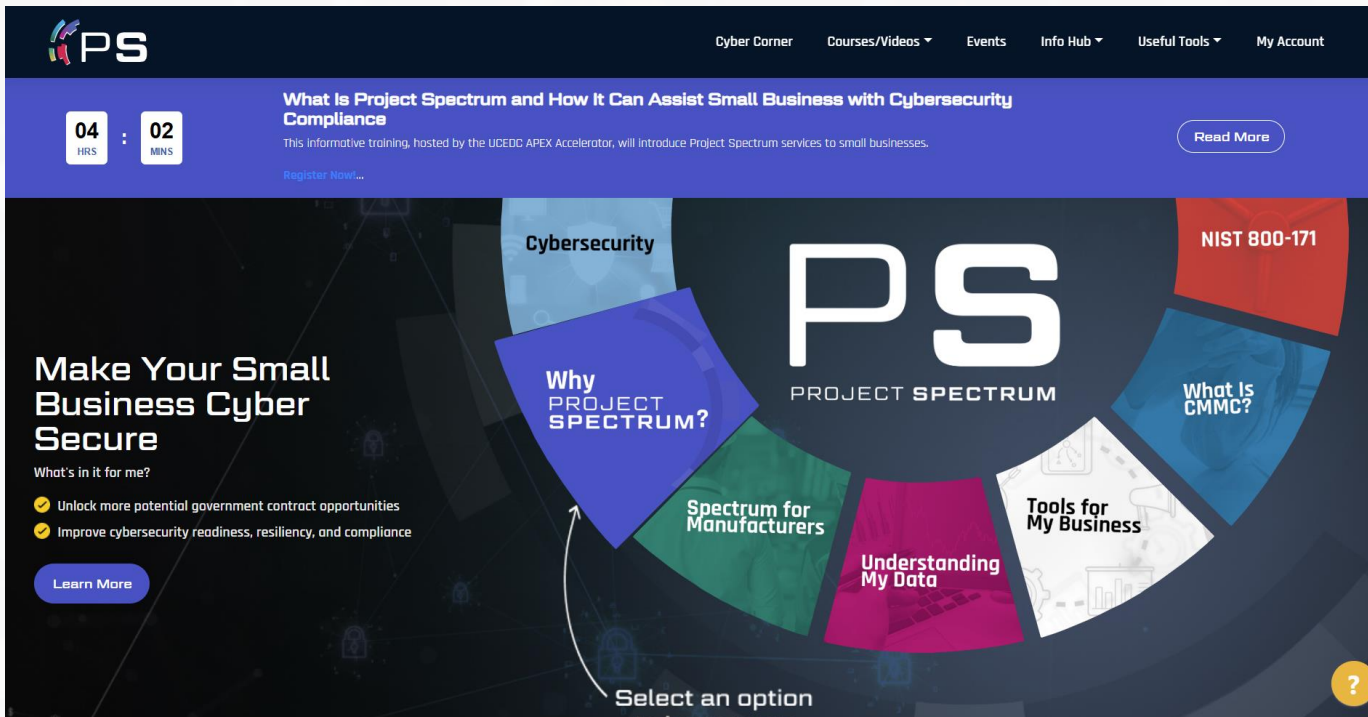
Stacy Bostjanick

Chief Defense Industrial Base
Cybersecurity and Deputy
CIO for Cybersecurity, DoW,
In an interview with GovCIO
Media & Research

“We are losing our intellectual property and sensitive data from the government by leaps and bounds. [Approximately] \$200 to \$600 billion a year in IP ... is lost, and sadly, many of our citizens are unaware.”



Project Spectrum Resources



The screenshot shows the Project Spectrum website home page. At the top, there is a navigation bar with links for Cyber Corner, Courses/Videos, Events, Info Hub, Useful Tools, and My Account. Below the navigation bar, there is a featured article titled "What is Project Spectrum and How It Can Assist Small Business with Cybersecurity Compliance" with a "Read More" button. The main content area features a large "PS PROJECT SPECTRUM" logo in the center, surrounded by several colorful circular buttons representing different resources: "Cybersecurity", "NIST 800-171", "What Is CMMC?", "Tools for My Business", "Understanding My Data", "Spectrum for Manufacturers", and "Why PROJECT SPECTRUM?". On the left side, there is a section titled "Make Your Small Business Cyber Secure" with a "Learn More" button and a list of benefits: "Unlock more potential government contract opportunities" and "Improve cybersecurity readiness, resiliency, and compliance".

Artifacts, Assessment Tools, and Advisory Services

- Security System Plans (SSP) Template
- Plans of Action and Milestones (POA&M)
- One-on-One Cyber Advisory Services
- Self-Assessment Toolkit
- Cyber Readiness Dashboard
- SPRS Score Generation and Uploads
- Remediation Plan Template

Education and Information Services

- Cybersecurity Training and Education
- Cybersecurity Blogs
- Cybersecurity News Items
- Project Spectrum Briefings

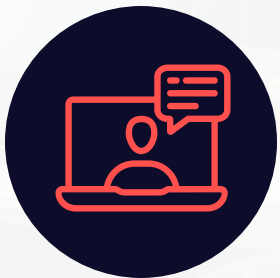
Connect With Project Spectrum



ProjectSpectrum.io



Support@ProjectSpectrum.io



Training Webinars



Social Media



Project Spectrum



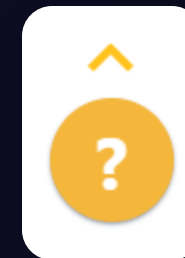
Project Spectrum



Introducing the Virtual Help Desk

Project Spectrum's new Virtual Help Desk gives visitors another way to reach our expert team of Cyber Advisors.

Clicking the orange question mark in the bottom right-hand corner of ProjectSpectrum.io will connect you with one of our Cyber Advisors.



The screenshot shows a 'Help' form with the following fields and elements:

- Summary ***: A text input field.
- What do you need help with? Provide as much detail as possible ***: A larger text input field.
- Your contact e-mail ***: A text input field.
- Send**: A blue button.
- Powered by Jira Service Management**: Text at the bottom of the form.