



Defending Your Business in Cyberspace

SOFWERX - Small Business Bootcamp 5

Presenter: Kareem A. Sykes

Date: March 12, 2025



MEET THE PRESENTER



Mr. Kareem A. Sykes

Project Spectrum
Industry & Engagement, Program Manager
Eccalon, LLC

Project Spectrum is a Department of Defense (DoD) recognized cybersecurity awareness initiative that provides the tools and training needed to increase cybersecurity awareness and maintain compliance in accordance with DoD 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

- 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

OVERVIEW OF THE CYBER THREAT LANDSCAPE & FEDERAL REGULATIONS



ABOUT PROJECT SPECTRUM

Project Spectrum Bolsters Homeland Defense

The DoD 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 DoD 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.
- Protects the homeland 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

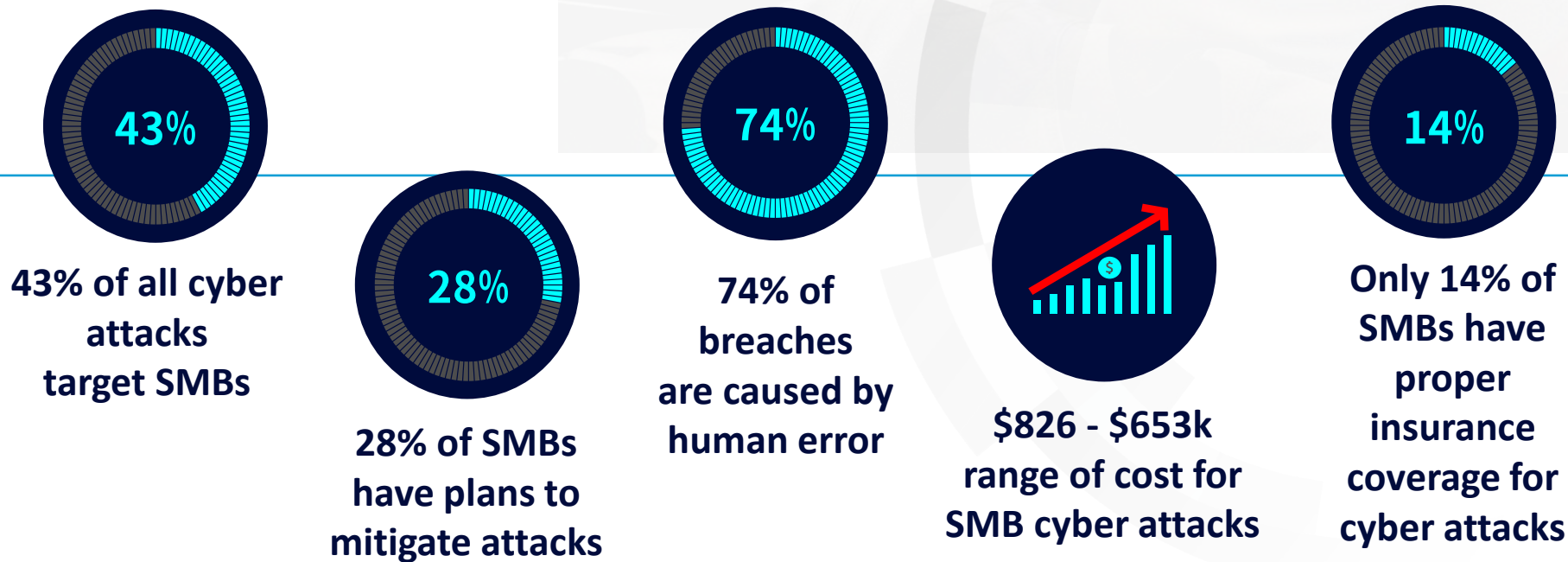
15 U.S.C. § 638 note

10 U.S.C. § 4901 note



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
- Access to sensitive government information
- Interconnection with larger defense contractors
- Access to the 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.

Controlled Unclassified Information (CUI)

DFARS Clause “252.204-7012”

CUI is a broad category of sensitive information, while unclassified, that requires safeguarding and dissemination of security controls pursuant to federal laws, regulations, and policies.



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.
- Estimates show **~50% of espionage within U.S. manufacturing is due to some sort of FOCI.**
- **FY 2023 NDAA Section 875** requires DoD 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 as “**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 CUI “prioritized” and “non-prioritized” data acquisitions.
- **CMMC Level 3** is considered as “**Expert**” for high capacity in safeguarding CUI data that is handled by the highest priority DoD programs.

CMMC Model	Model	Assessment
LEVEL 3	24 requirements aligned with NIST 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 is required.
- To be compliant, the contractor needs all findings to result in a **“Met”** or **“N/A”** status. 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 has a **bifurcation or split** that occurs towards DIB contractors that handle CUI data acquisitions. There are two compliance tracks. Each requiring a minimum passing score of 88 of out 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 assessors.
- 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 (cont.)

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

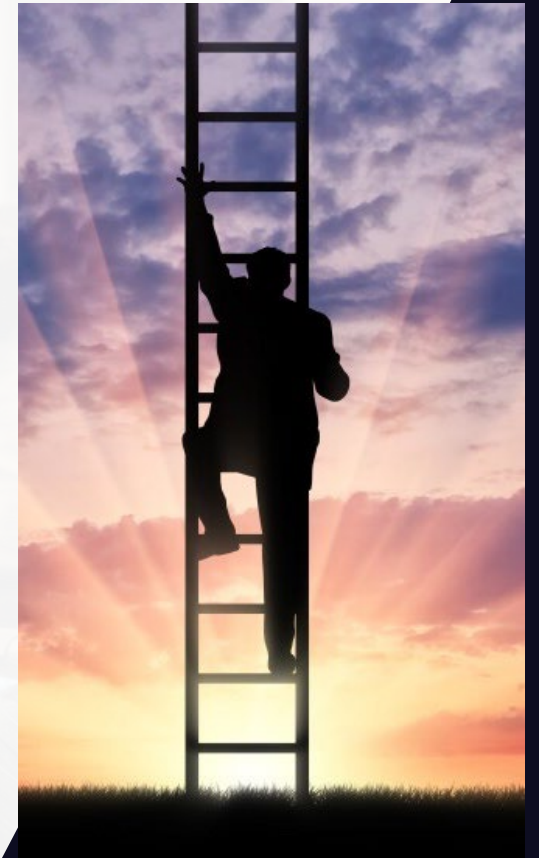
If the CUI data that your company handles, falls into the following category data types, your company will need to be assessed by a CMMC Third Party Assessment Organization (C3PAO) to achieve CMMC Level 2 Certification.

Defense:

- Controlled Technical Information
- DoD 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-Requisite:** 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 DoD CUI Registry by visiting <https://www.dodcui.mil/CUI-Registry-New/>

STEP 2 – Conduct a CMMC Level 1 Self-Assessment Scope

Within the Project Spectrum platform, a CMMC Level 1 Scoping Assessment tool 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 CMMC Level 1 Scoping Assessment tool interface. The header includes the Project Spectrum logo and navigation links: Home, Courses, Events, Partners, Info Hub, Resources, and Contact Us. The main title is "CMMC Level 1 Scoping Assessment" with a sub-header "Page 1 of 1". The form contains four sections:

- 1. CURRENT CONTRACTS: Do you have any current contracts that contain Federal Contract Information (FCI) protection requirements? ***
☒ Yes ☐ No
- 2. List & Describe any contracts containing FCI protection requirements.**
DoD Contract #: -----
Purpose: to provide front office support for the Project Management Office and to provide strategic planning.
- 3. PENDING CONTRACTS: Are you currently pursuing contracts that contain FCI protection requirements? ***
☒ Yes ☐ No
- 4. List & Describe any contracts you are pursuing that contain FCI protection requirements. ***
DoD Contract #: -----
We are pursuing a software development contract designed to provide Agency ABC with a platform for

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 Level 1 Self-Assessment

The Project Spectrum Self-Assessment tool is used to examine how a company is safeguarding FCI 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)

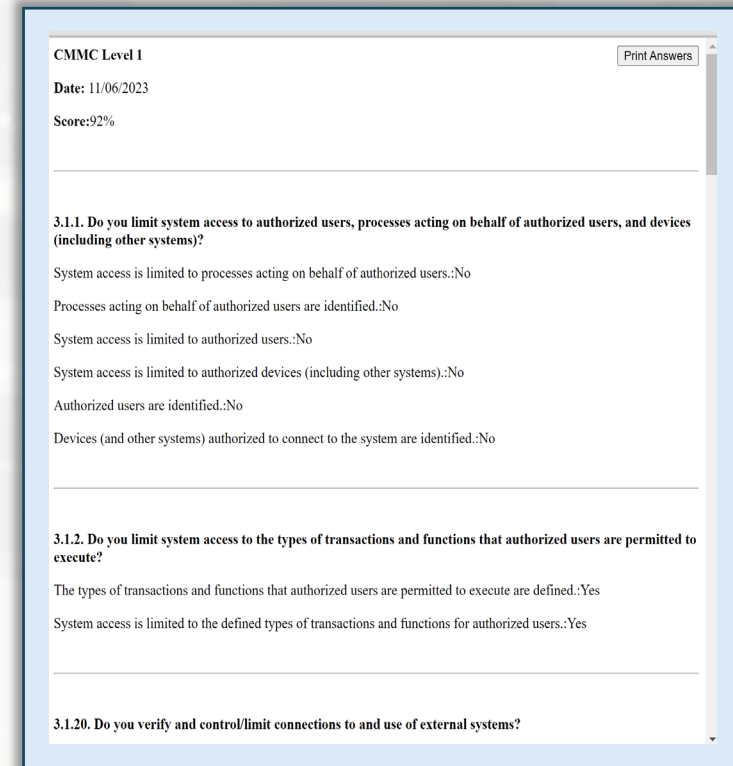
[CMMC Self-Assessment Guide \(Level 1\)](#)

The screenshot shows the 'CMMC Level 1 Self Assessment' interface. At the top is a navigation bar with the 'PS' logo and links for 'Cyber Corner', 'Courses/Videos', 'Events', 'Info Hub', 'Useful Tools', 'Speaker Request', and 'My Account'. The main heading is 'CMMC Level 1 Self Assessment' with a sub-heading 'Introduction to Level 1 Self-Assessment'. Below this, it lists 'Access Control (AC) A.C.L.1-B.1.1 - AUTHORIZED ACCESS CONTROL' and 'A.C.L.1-B.1.1 - AUTHORIZED ACCESS CONTROL [Federal Contract Information (FCI) DATA]'. The text describes the requirement to 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' (Access control policy, System configuration settings, List of authorized users and devices), and an 'Example' (Maintain a list of employees with access to company computers). At the bottom, there is a section titled '1. A.C.L.1-B.1.1 - AUTHORIZED ACCESS CONTROL [FCI DATA] *' with a description and four questions, each with four radio button options: 'Yes', 'No', 'Not Applicable', and 'Answer Later'. The questions are: 'Authorized users are identified?', 'Processes acting on behalf of authorized users are identified?', 'Devices (and other systems) authorized to connect to the system are identified?', and 'System access is limited to authorized users?'.

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



The screenshot displays a web-based assessment interface for CMMC Level 1. At the top, it shows 'CMMC Level 1', a 'Date: 11/06/2023', and a 'Score: 92%'. A 'Print Answers' button is in the top right corner. The main content area lists three questions with their corresponding answers:

- 3.1.1. Do you limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems)?**
System access is limited to processes acting on behalf of authorized users.:No
Processes acting on behalf of authorized users are identified.:No
System access is limited to authorized users.:No
System access is limited to authorized devices (including other systems):.No
Authorized users are identified.:No
Devices (and other systems) authorized to connect to the system are identified.:No
- 3.1.2. Do you limit system access to the types of transactions and functions that authorized users are permitted to execute?**
The types of transactions and functions that authorized users are permitted to execute are defined.:Yes
System access is limited to the defined types of transactions and functions for authorized users.:Yes
- 3.1.20. Do you verify and control/limit connections to and use of external systems?**

STEP 5 – Develop a Remediation Plan

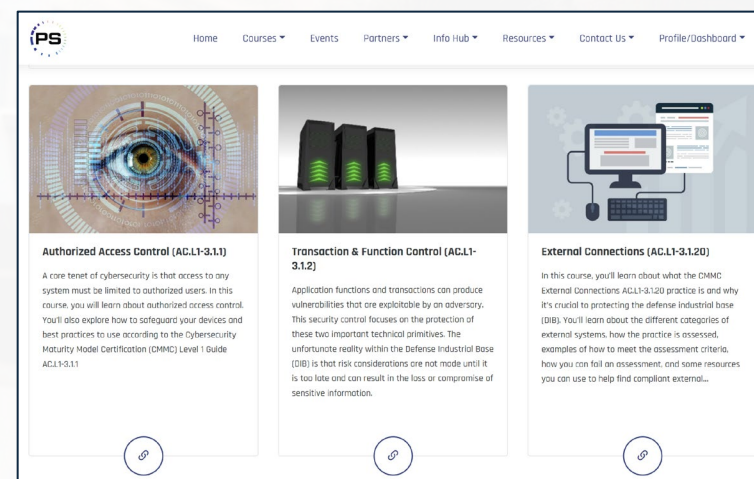
A remediation plan is developed to address and rectify identified security gaps, deficiencies, or vulnerabilities within an organization's cybersecurity controls. It outlines the specific actions, resources, timelines, and steps necessary to close these gaps and enhance security.



- 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

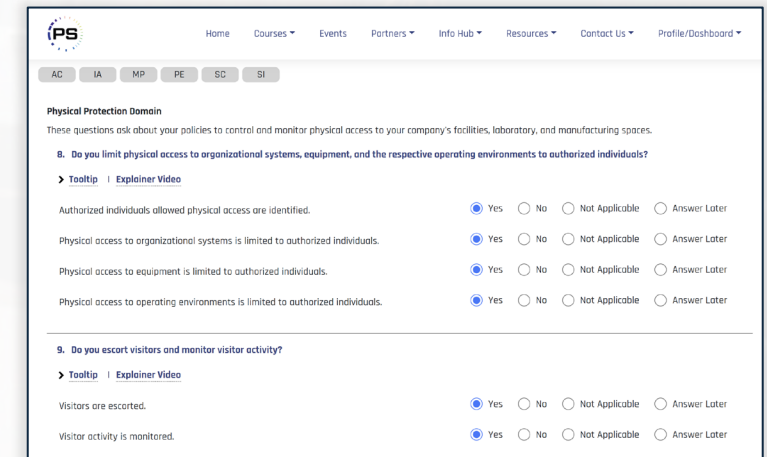
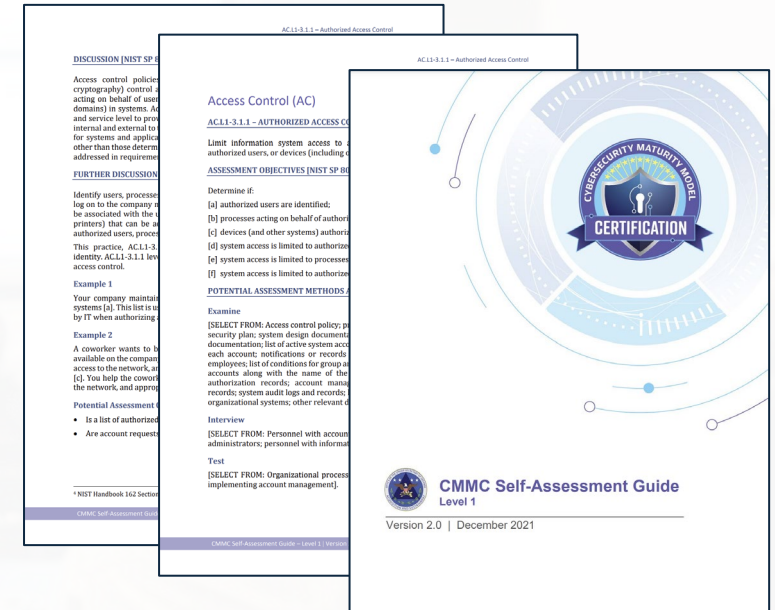


COMPLIANCE SCENARIO

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 DoD 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 with their journey **at no cost** to the business.



outreach@projectspectrum.io

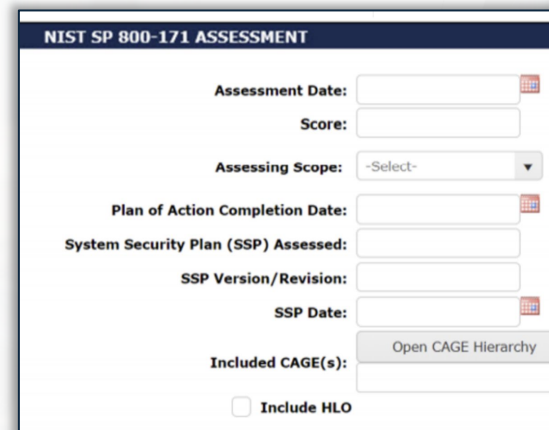
COMPLIANCE SCENARIO

STEP 8 – Upload Results to SPRS

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

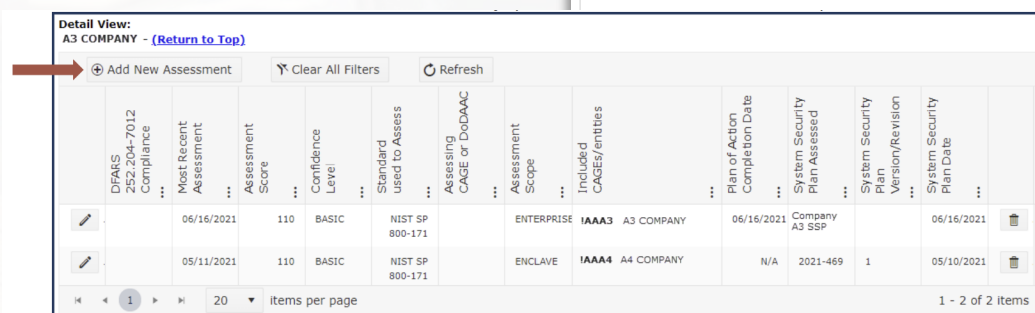
SPRS Website: [Supplier Performance Risk System](#)

- 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



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.



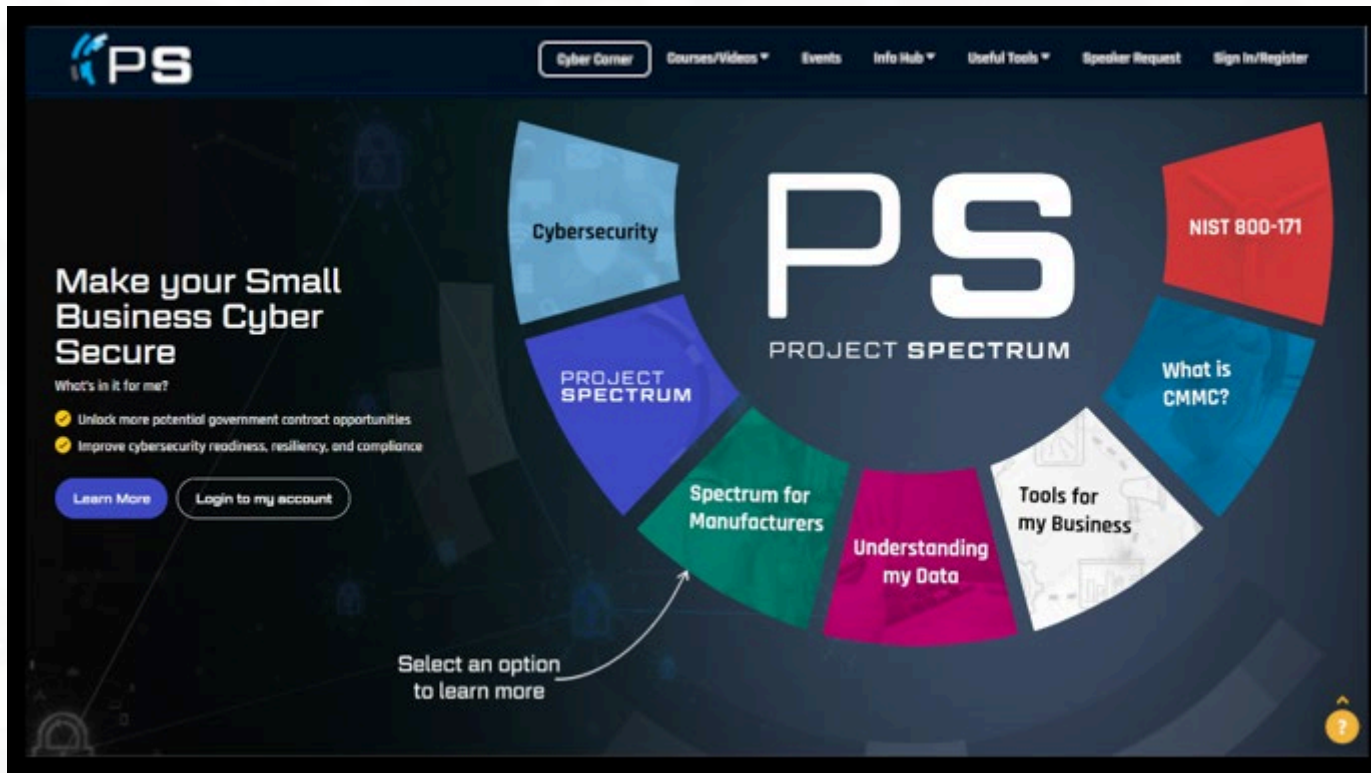
Detail View: A3 COMPANY - (Return to Top)													
Add New Assessment Clear All Filters Refresh													
	DFARS 252.204-7012 Compliance	Most Recent Assessment	Assessment Score	Confidence Level	Standard used to Assess	Assessing CAGE or DoDAAC	Assessment Scope	Included CAGE/entities	Plan of Action 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



Project Spectrum Resources



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

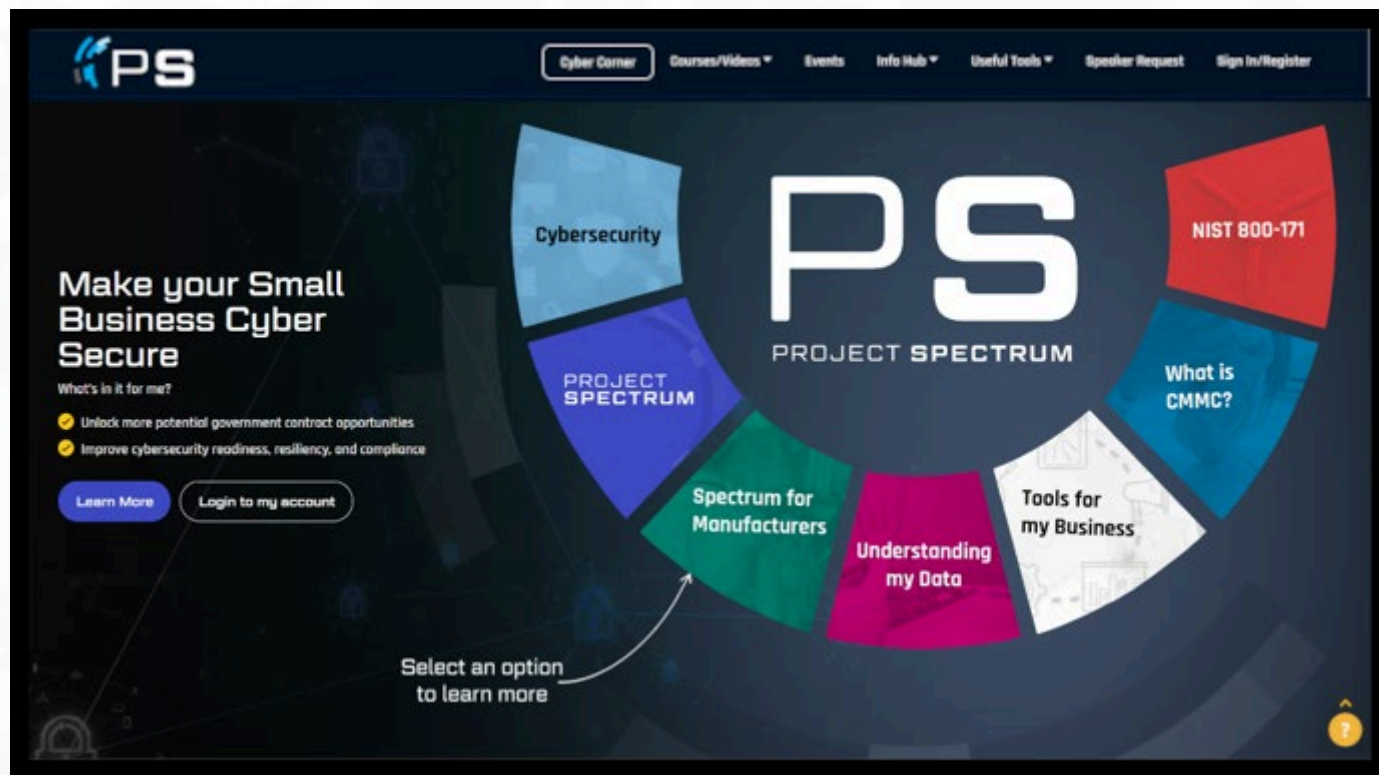
Education and Information Services

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

INTRODUCING THE LATEST

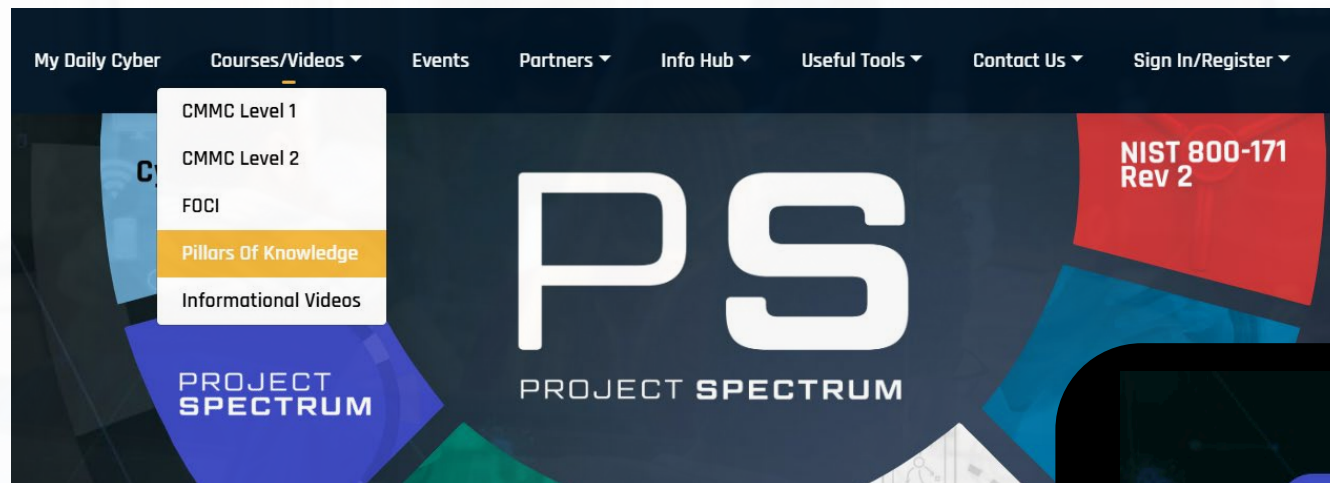
ProjectSpectrum.io Portal

The newest iteration of ProjectSpectrum.io introduces a few notable new features:



- Customized Roadmaps
- Short Informative Videos on Cybersecurity
- “Pillars of Knowledge”
- New ‘Micro Lessons’
- Virtual Help Desk

Pillars of Knowledge



These Pillars of Knowledge focus on key areas of cybersecurity

This section of site features short informative videos focused on these topics



ProjectSpectrum.io: Informative Videos

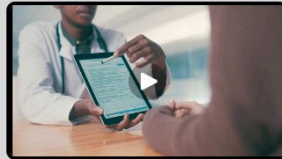
The Informative Videos area of the site features a series of short, informative videos, that cover foundational cybersecurity practices in a matter of minutes.

These videos compliment Project Spectrum courses on a range of topics including:

- Cybersecurity Kill Chain
- Manufacturing Vulnerabilities
- Strategies of Readiness
- Industry Forecasting
- Identifying Data Types



SpectrumManufacturers
Manufacturing Vulnerabilities
Protect your operations and facilities



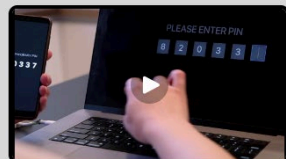
UnderstandingData
Identify Data Types

Define the types of data the business will collect, process, and store



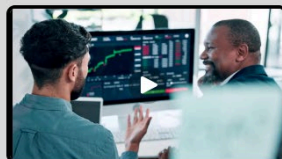
UnderstandingData
Decision Making

Consider data analysis and visualization techniques to draw conclusions from your data



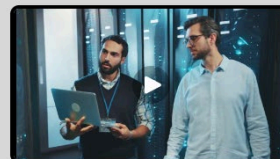
UnderstandingData
Implementation

Implement governance procedure for quality, security, and compliance



BusinessTools
Essential Requirements

Determine your company's unique requirements and objectives



BusinessTools
Equip Yourself

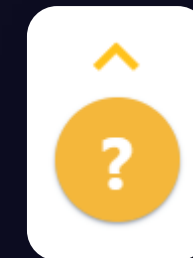
Research and evaluate tools specific to your industry and business size



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.



Help

×

Summary *

What do you need help with? Provide as much detail as possible *

Your contact e-mail *

Send

Powered by Jira Service Management

The Benefits You Get with Project Spectrum

- **World-class team of Cyber Advisors with expertise** rooted in cybersecurity for small and medium-sized businesses
- **Expert cybersecurity practitioners** with government and/or industry experience
- **Sponsored and endorsed by the DoD Office of Small Business Programs**
- **Self-paced tools, training, and resources** for novices and experts alike
- Services provided at **no cost to the user**

Best in Class Cybersecurity Training and Resources

- Full-Scope Training courses focused on: CUI for Contractors, Plan of Actions & Milestones, CMMC Level 1, and Systems Security Plan Fundamentals
- 26 'micro-courses' that provide training on core CMMC controls
- DIY tools enabling companies to conduct self-assessments against NIST and CMMC standards
- Strategic Partnerships with the DoD Mentor-Protégé Program
- Community Outreach & Engagement

Connect With Project Spectrum



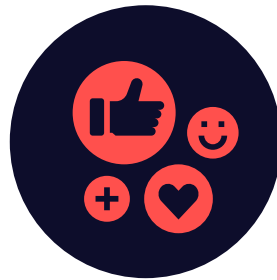
ProjectSpectrum.io



Support@ProjectSpectrum.io



Training Webinars



Social Media



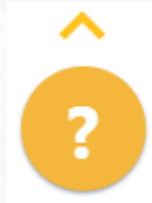
Project Spectrum



Project Spectrum

Don't hesitate! Connect with Project Spectrum today by registering at [Projectspectrum.io](https://projectspectrum.io)

Once registered, you can reach our Cyber Advisory Team by clicking on

A screenshot of a web form titled "Help" with a close button (X) in the top right corner. The form contains three input fields: "Summary*", "What do you need help with? Provide as much detail as possible*", and "Your contact e-mail*". Below the third field is a blue "Send" button. At the bottom of the form, it says "Powered by Jira Service Management".

QUESTIONS

