PROJECT SPECTRUM

Defending Your Small Business in Cyberspace

Speaker: Mr. Kareem Sykes
Project Spectrum
Industry & Engagement Manager

27 March 2024

DEPARTMENT OF DEFENSE
OFFICE OF SMALL BUSINESS PROGRAMS

EDUCATION: Helping Businesses with Cybersecurity

Educate businesses on the landscape of Cybersecurity Threats

Educate businesses that nation-states and sophisticated hackers are indeed targeting even the smallest of businesses if they are handling sensitive government information.

Provide an overview on Federal regulations for safeguarding data and information

Give businesses data and guidance on the regulations they are obligated to comply with to obtain DoD contracts, to help protect proprietary and Government data, and to improve cybersecurity.

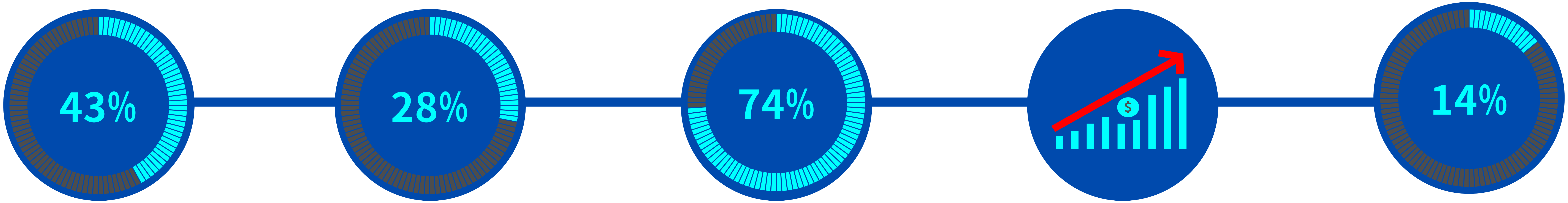
Brief businesses on the CMMC process

Provide businesses an overview of the CMMC, scope and gap assessments, required documentation, self attestation, SPRS scores, and how to get certified.

Provide an overview on how Project Spectrum can help with the CMMC journey

Educate businesses on the services provided by Project Spectrum, how they can use those services to reduce or eliminate costs related to CMMC compliance, and how to improve their cybersecurity posture.

EDUCATION: Threat Landscape



of all cyber attacks target SMBs

of SMBs have plans to mitigate attacks

of breaches are caused by human error

$826 - $653k range of cost for SMB cyber attacks

of SMBs have the proper insurance coverage to cover cyber attacks

WHY ARE SMBs BEING TARGETED?

Intellectual property

Access to sensitive Government information

Interconnection with larger defense contractors

Access to the supply chain

Political and ideological motivation

UNDERSTANDING FCI & CUI DATA

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 is a subset of CUI.

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.

PROJECT SPECTRUM

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

- FOCI is a state that many 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:

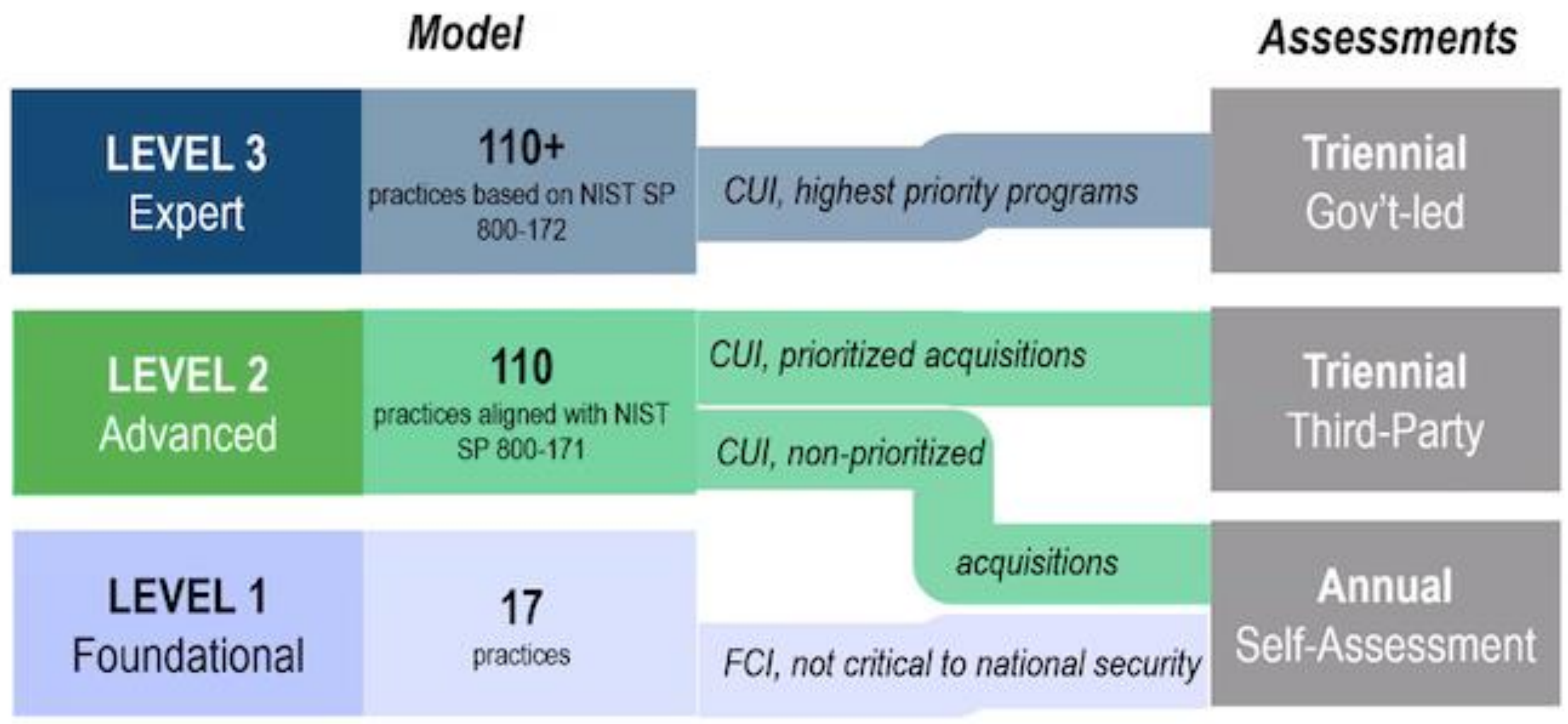
- Properly identifying FOCI
- Evaluating the impact of FOCI
- Reducing FOCI risks

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 in which this type carries the highest priority DoD programs.



Model			Assessments
LEVEL 3 Expert	110+ practices based on NIST SP 800-172	CUI, highest priority programs	Triennial Gov't-led
LEVEL 2 Advanced	110 practices aligned with NIST SP 800-171	CUI, prioritized acquisitions	Triennial Third-Party
		CUI, non-prioritized acquisitions	
LEVEL 1 Foundational	17 practices	FCI, not critical to national security	Annual Self-Assessment

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.
- Self-assessments 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 ensures a **bifurcation or split** that occurs towards DIB contractors that handle either "prioritized" and/or "non-prioritized" CUI data acquisitions.

Split-a: "Non-prioritized" or less sensitive CUI data acquisitions:

- **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).

Split-b: "Prioritized" or sensitive CUI data acquisitions:

- **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.

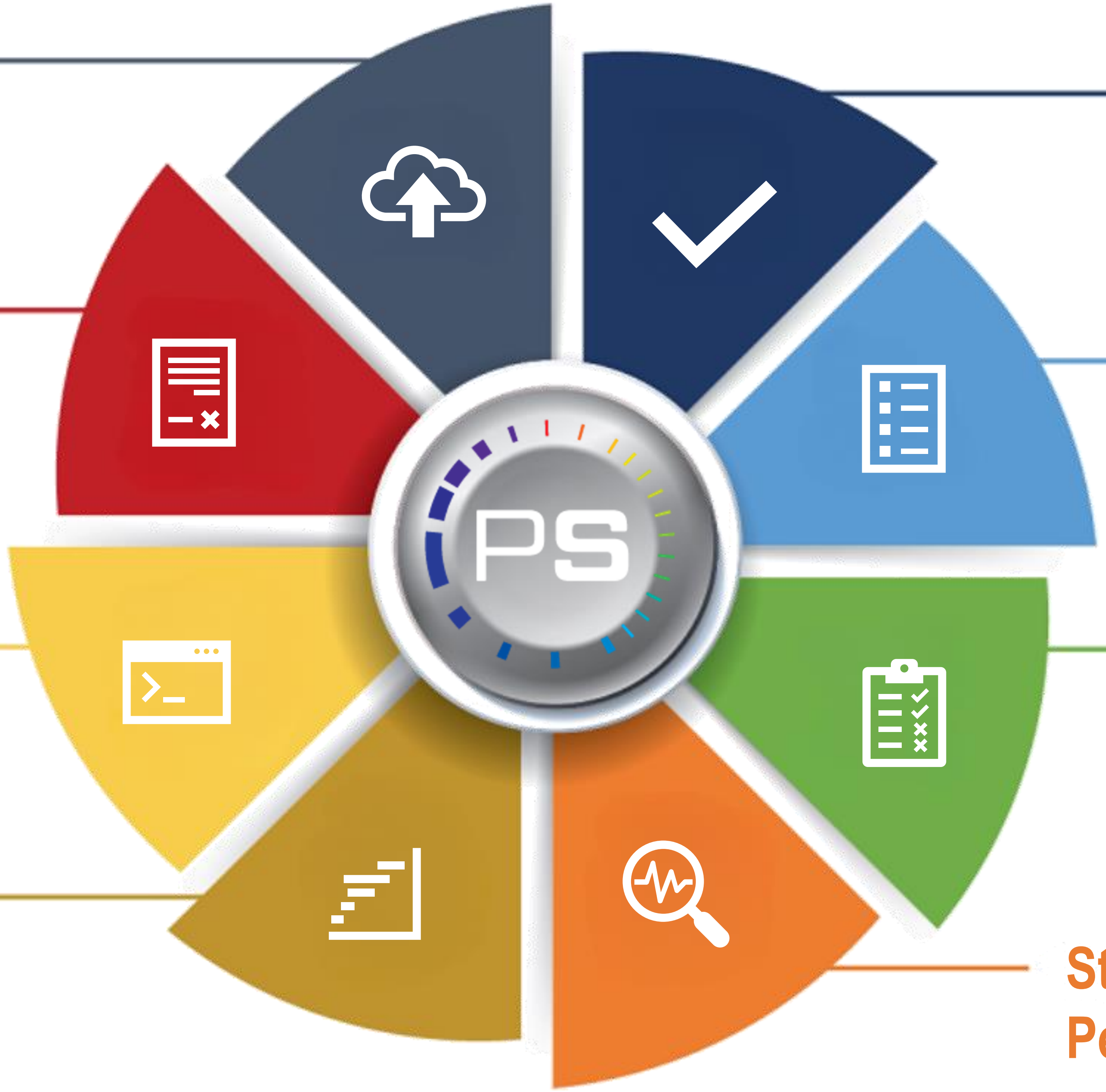
ASSESSMENT REQUIREMENTS: CMMC Level 3

- A triennial (every 3-year cycle) assessment and certification renewal is required
- Government officials will conduct the assessment:
  - Defense Contract Management Agency “DCMA - DIBCAC”

Compliance Scenario
CMMC Level 1

Process overview for meeting CMMC Level 1 compliance requirements utilizing Project Spectrum

Compliance Scenario – CMMC Level 1



Step 1:
Select appropriate CMMC level

Step 2:
Conduct scoping assessment

Step 3:
Conduct self-assessment

Step 4:
Perform gap analysis

Step 5:
Develop remediation plan

Step 6:
Implement security controls

Step 7:
Prepare documentation and evidence

Step 8:
Upload self-assessment to SPRS

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.

Controlled
Unclassified
Information

Federal Contract Information (FCI) Data

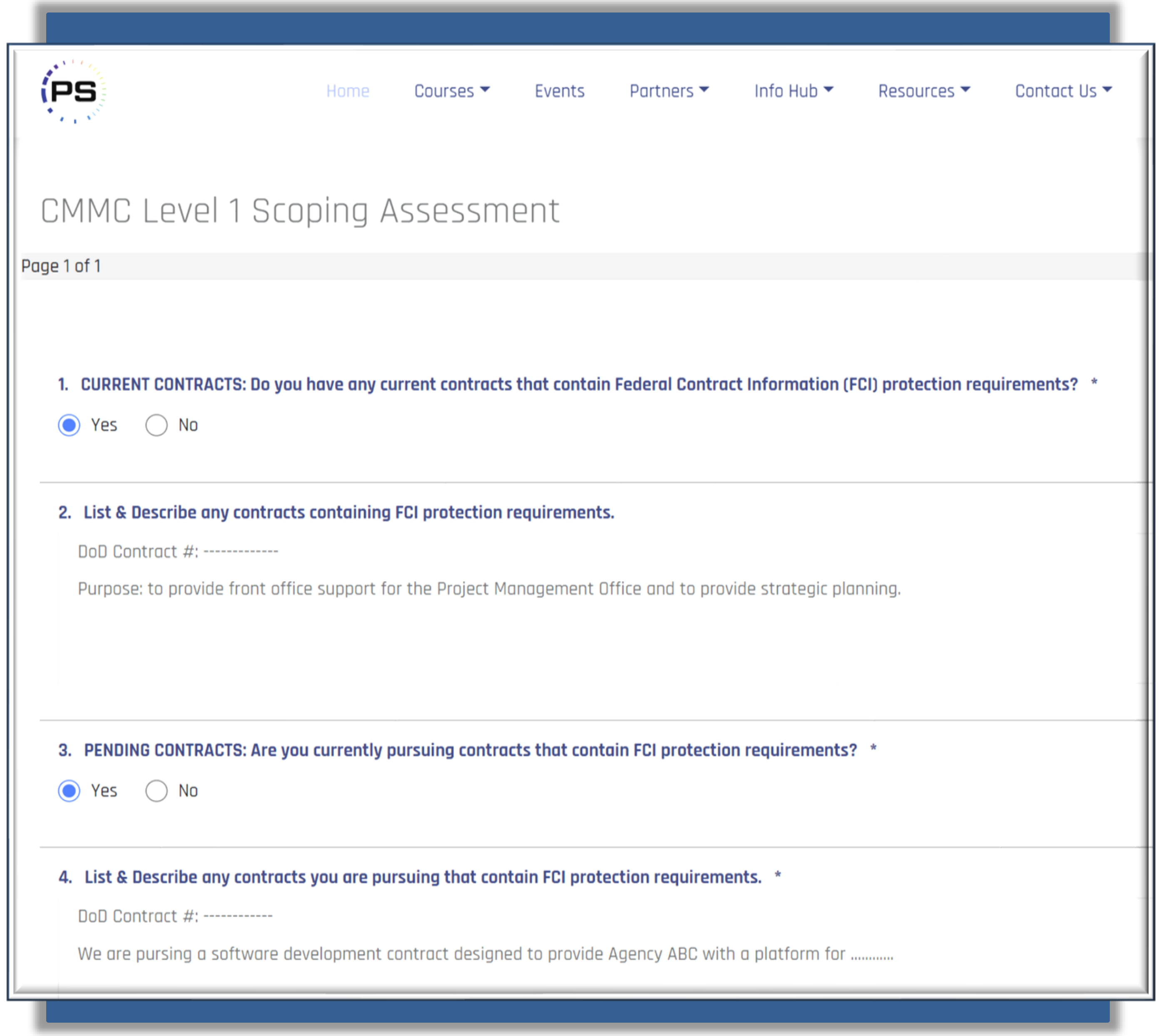
Data generated for the Federal Government under a contract to develop or deliver a product or service and is not intended for public release.

Controlled Unclassified Information (CUI) Data

Information that requires safeguarding and may also be subject to dissemination controls.

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.



CMMC Level 1 Scoping Assessment

Page 1 of 1

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 pursing 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
- 51 questions

Scoping for CMMC Level 2

CMMC Level 2 Scoping Documentation

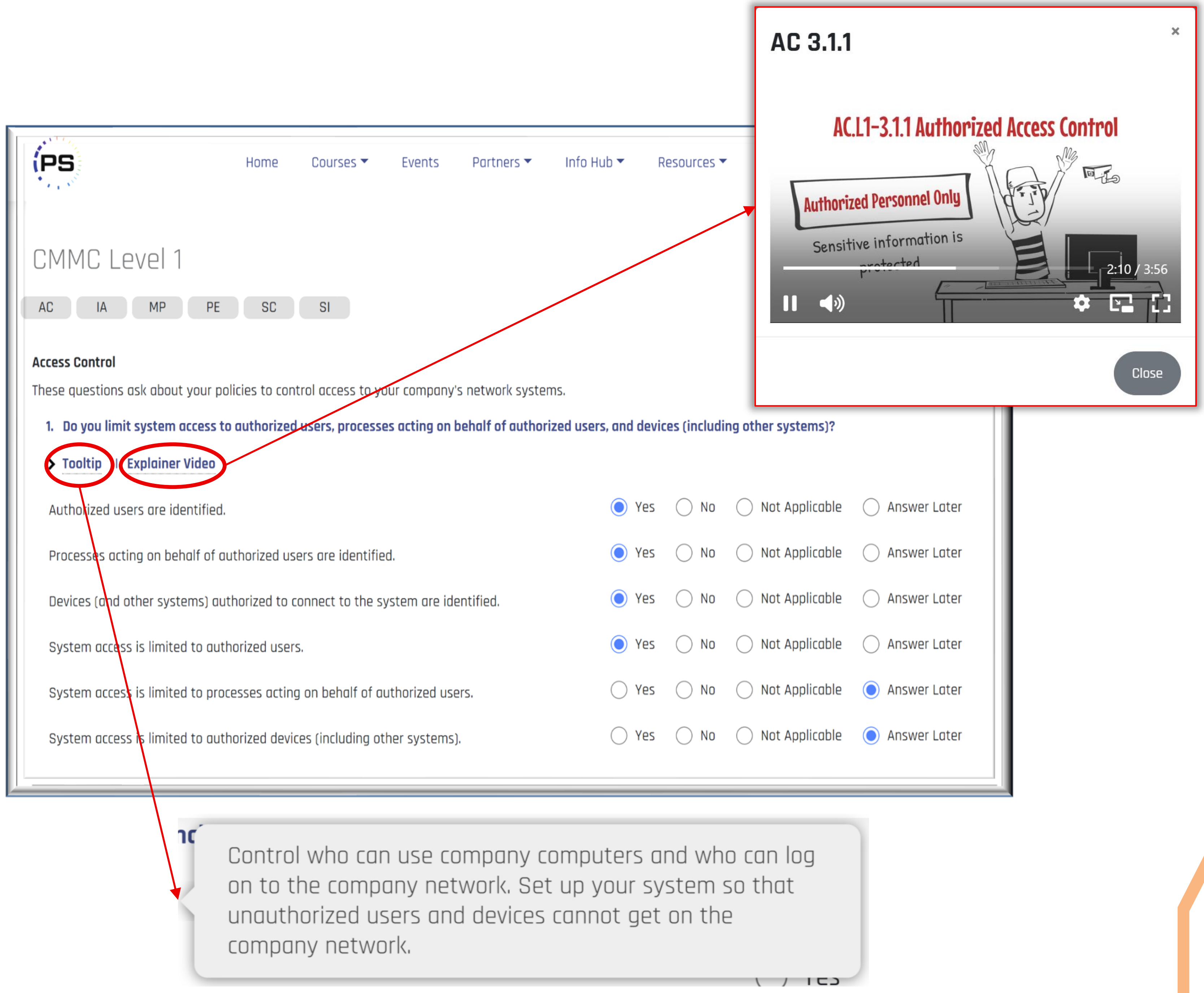
- Focus on CUI assets
- Covers 14 family domains
- 69 questions
- Must produce System Security Plans (SSP) and Plan of Actions & Milestones (POA&M) documentation

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 Provide (ESP)
- 6 Family Domains and 17 Practices

[CMMC Self-Assessment Guide (Level 1)]


PS
Home
Courses
Events
Partners
Info Hub
Resources
AC
IA
MP
PE
SC
SI
AC 3.1.1
×
AC.L1-3.1.1 Authorized Access Control
Authorized Personnel Only
Sensitive information is protected
2:10 / 3:56
Close

CMMC Level 1

Access Control

These questions ask about your policies to control access to your company's network systems.

1. Do you limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems)?

Tooltip | Explainer Video

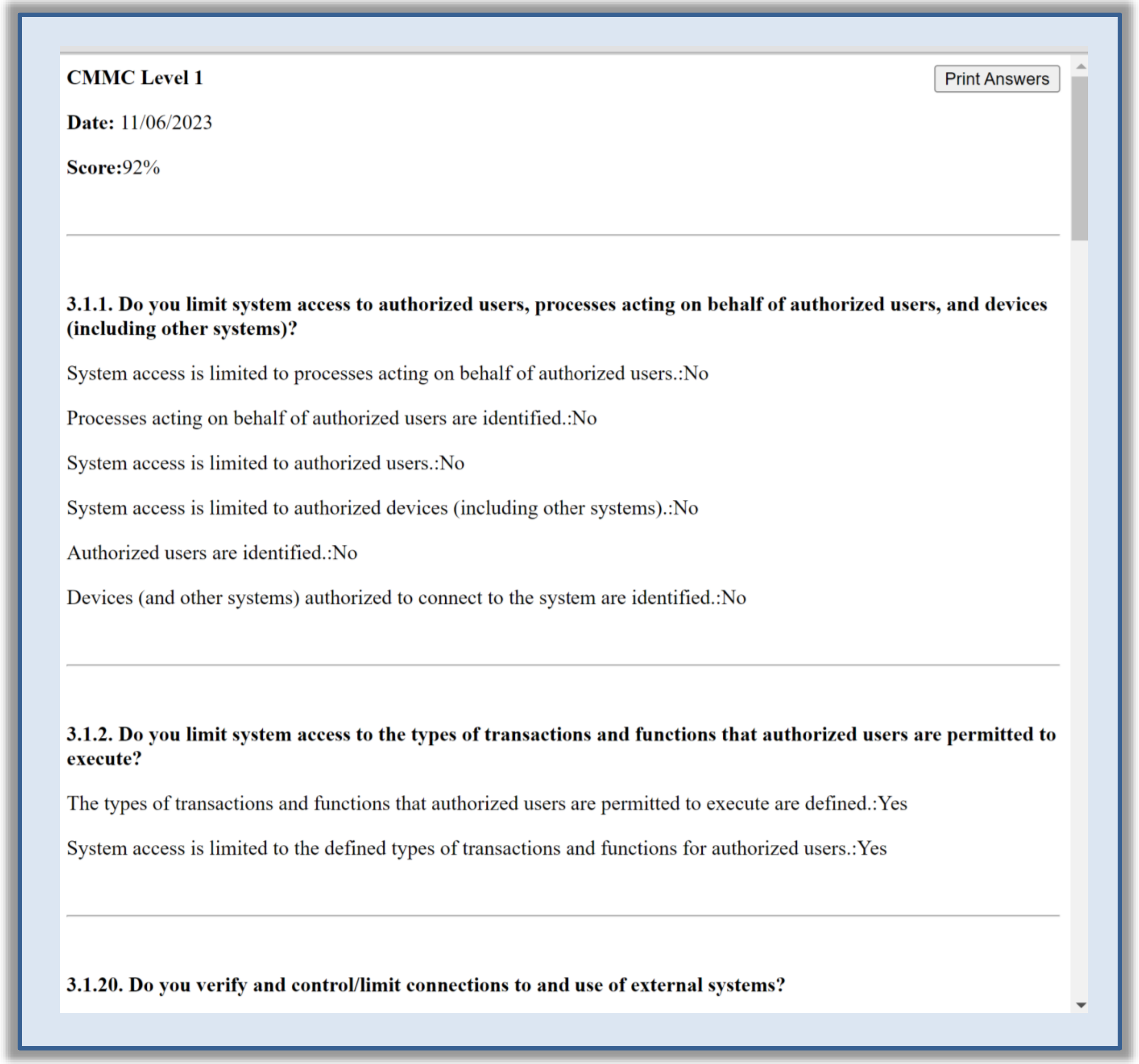
Authorized users are identified.	● Yes	○ No	○ Not Applicable	○ Answer Later
Processes acting on behalf of authorized users are identified.	● Yes	○ No	○ Not Applicable	○ Answer Later
Devices (and other systems) authorized to connect to the system are identified.	● Yes	○ No	○ Not Applicable	○ Answer Later
System access is limited to authorized users.	● Yes	○ No	○ Not Applicable	○ Answer Later
System access is limited to processes acting on behalf of authorized users.	○ Yes	○ No	○ Not Applicable	● Answer Later
System access is limited to authorized devices (including other systems).	○ Yes	○ No	○ Not Applicable	● Answer Later

Control who can use company computers and who can log on to the company network. Set up your system so that unauthorized users and devices cannot get on the company network.

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



CMMC Level 1

Date: 11/06/2023

Score:92%

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.

PROJECT SPECTRUM

Remediation Plan

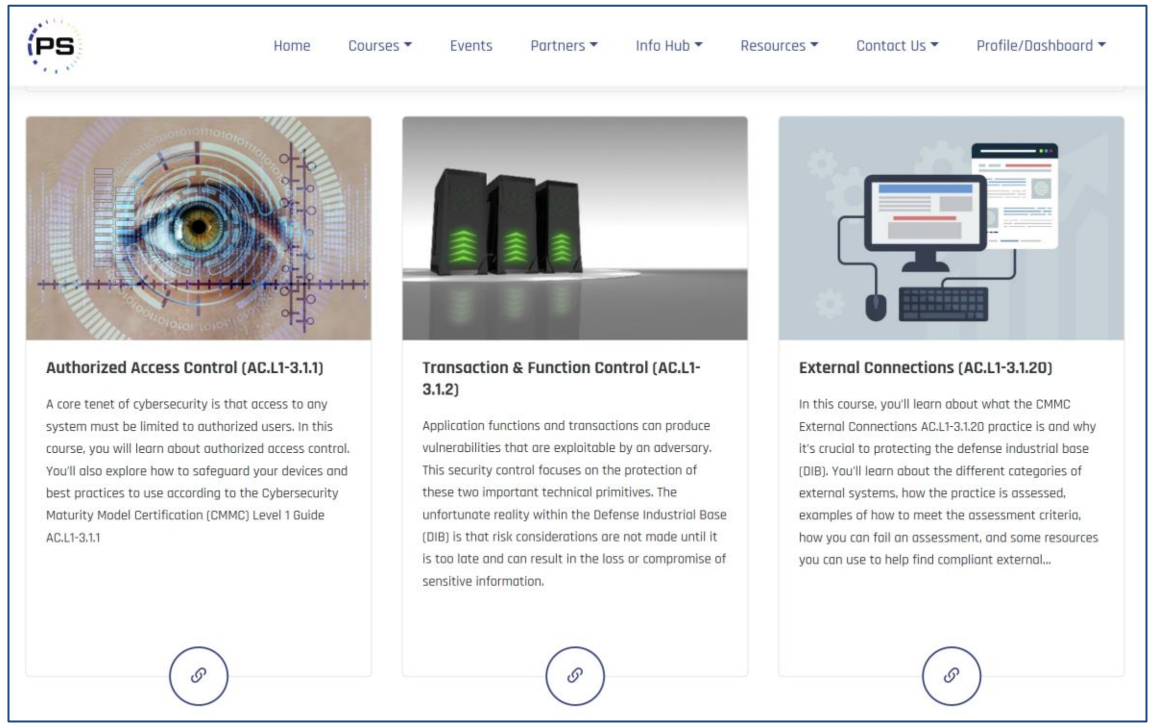
A Guide to Rectify Security Gaps

November 2023

- 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



Authorized Access Control (AC.L1-3.1.1)

A core tenet of cybersecurity is that access to any system must be limited to authorized users. In this course, you will learn about authorized access control. You'll also explore how to safeguard your devices and best practices to use according to the Cybersecurity Maturity Model Certification (CMMC) Level 1 Guide AC.L1-3.1.1

Transaction & Function Control (AC.L1-3.1.2)

Application functions and transactions can produce vulnerabilities that are exploitable by an adversary. This security control focuses on the protection of these two important technical primitives. The unfortunate reality within the Defense Industrial Base (DIB) is that risk considerations are not made until it is too late and can result in the loss or compromise of sensitive information.

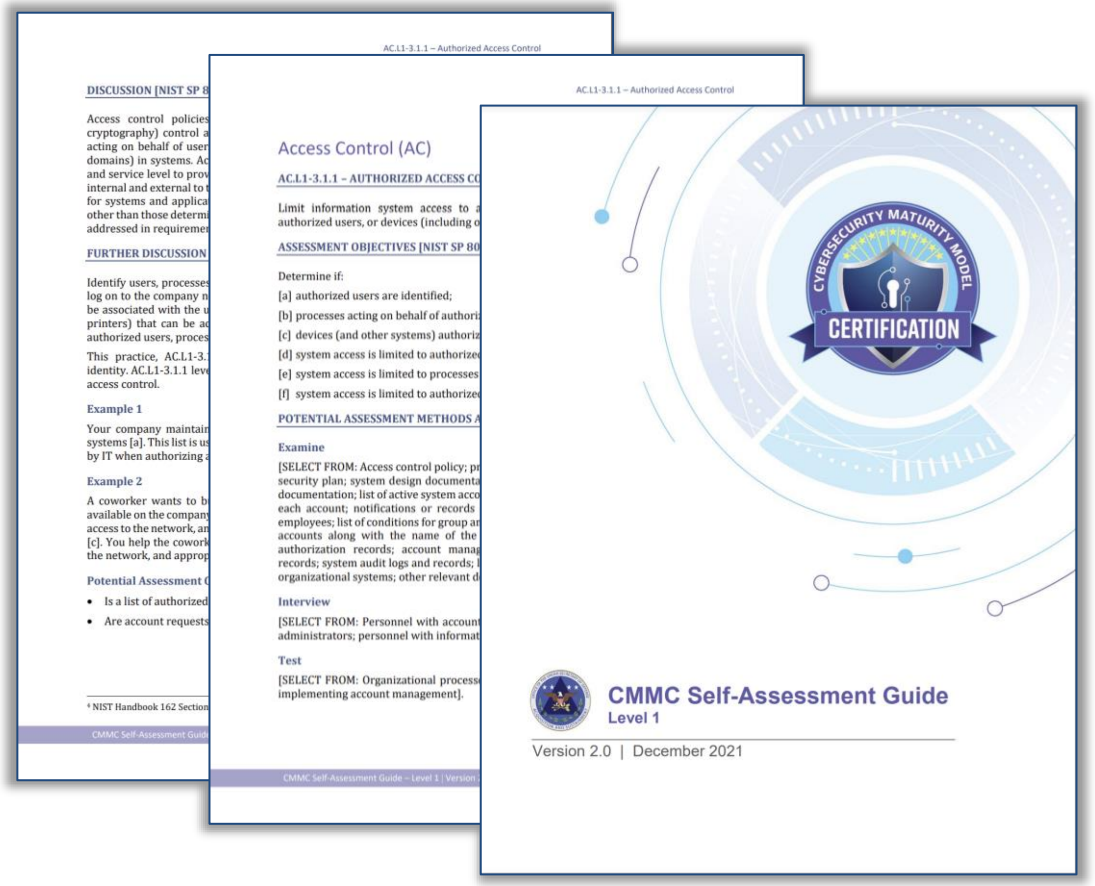
External Connections (AC.L1-3.1.20)

In this course, you'll learn about what the CMMC External Connections AC.L1-3.1.20 practice is and why it's crucial to protecting the defense industrial base (DIB). You'll learn about the different categories of external systems, how the practice is assessed, examples of how to meet the assessment criteria, how you can fail an assessment, and some resources you can use to help find compliant external...

STEP 6: Implement Security Controls

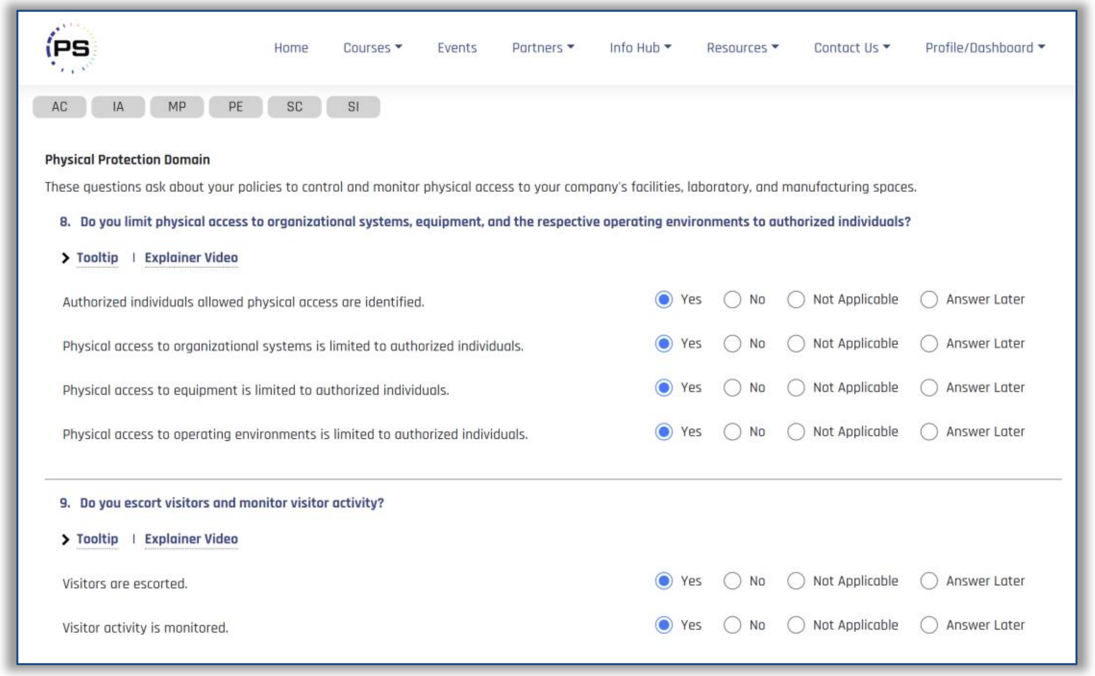
The implementation process is a critical step towards remediating the gaps that were found after conducting the self assessment process. Consider the following steps for the remediation plan and implementation process:

- 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


AC.L1-3.1.1 – Authorized Access Control
CYBERSECURITY MATURITY MODEL
CERTIFICATION

Access Control (AC)

CMMC Self-Assessment Guide
Level 1
Version 2.0 | December 2021



Physical Protection Domain

These questions ask about your policies to control and monitor physical access to your company's facilities, laboratory, and manufacturing spaces.

8. Do you limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals?

Authorized individuals allowed physical access are identified. ● Yes ○ No ○ Not Applicable ○ Answer Later

Physical access to organizational systems is limited to authorized individuals. ● Yes ○ No ○ Not Applicable ○ Answer Later

Physical access to equipment is limited to authorized individuals. ● Yes ○ No ○ Not Applicable ○ Answer Later

Physical access to operating environments is limited to authorized individuals. ● Yes ○ No ○ Not Applicable ○ Answer Later

9. Do you escort visitors and monitor visitor activity?

Visitors are escorted. ● Yes ○ No ○ Not Applicable ○ Answer Later

Visitor activity is monitored. ● Yes ○ No ○ Not Applicable ○ Answer Later

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

Network Topology
Internet
Desktop
Desktop
Hub
Router
Hub
Desktop
Desktop
Smartphone
Wireless Router
Laptop

PROJECT SPECTRUM

System Security Plan (SSP)
A Guide for CMMC Requirements

November 2023

PROJECT SPECTRUM

Incident Response Plan
A Guide for Responding
to Security Incidents

November 2023

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.

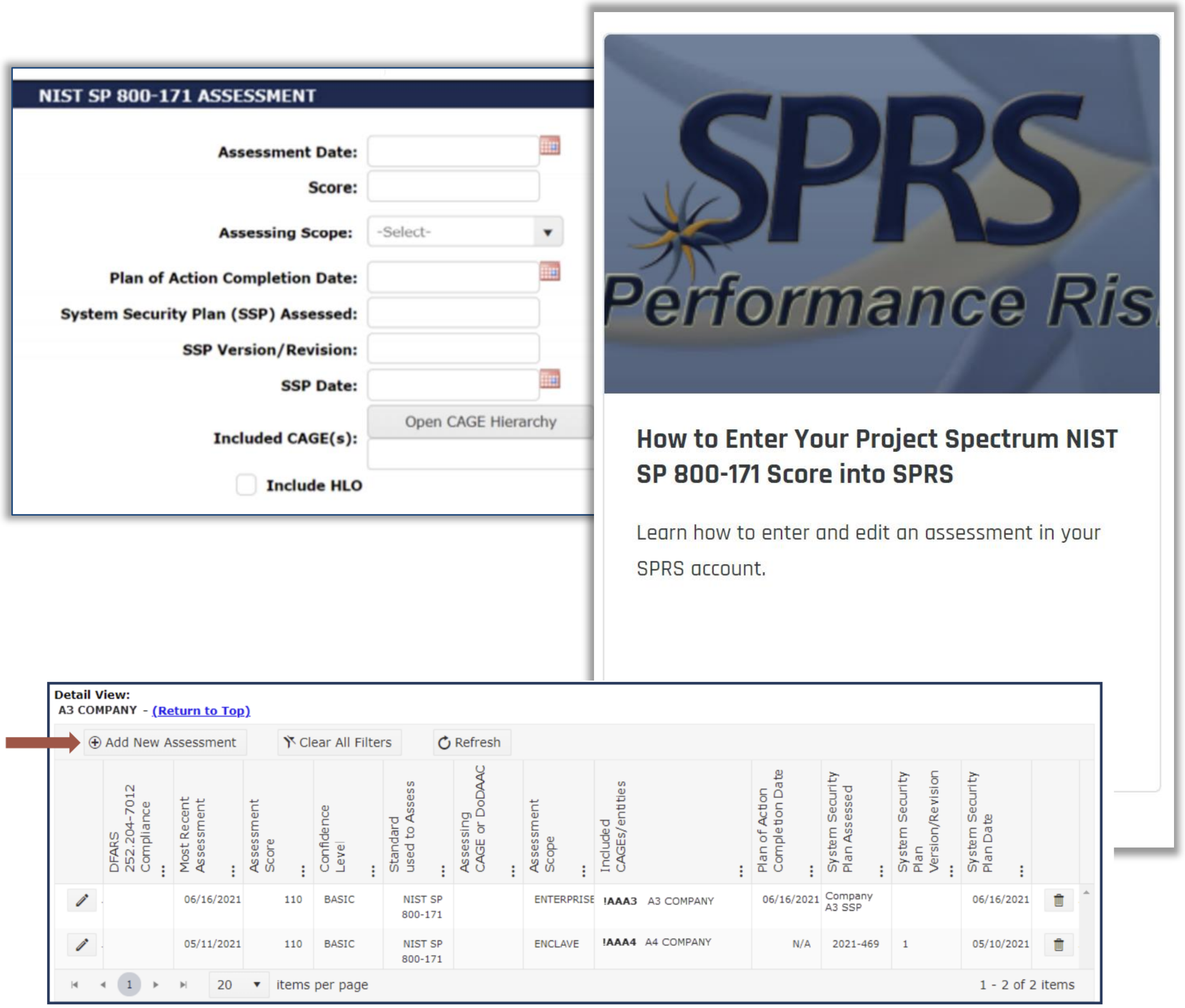
outreach@projectspectrum.io

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



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.

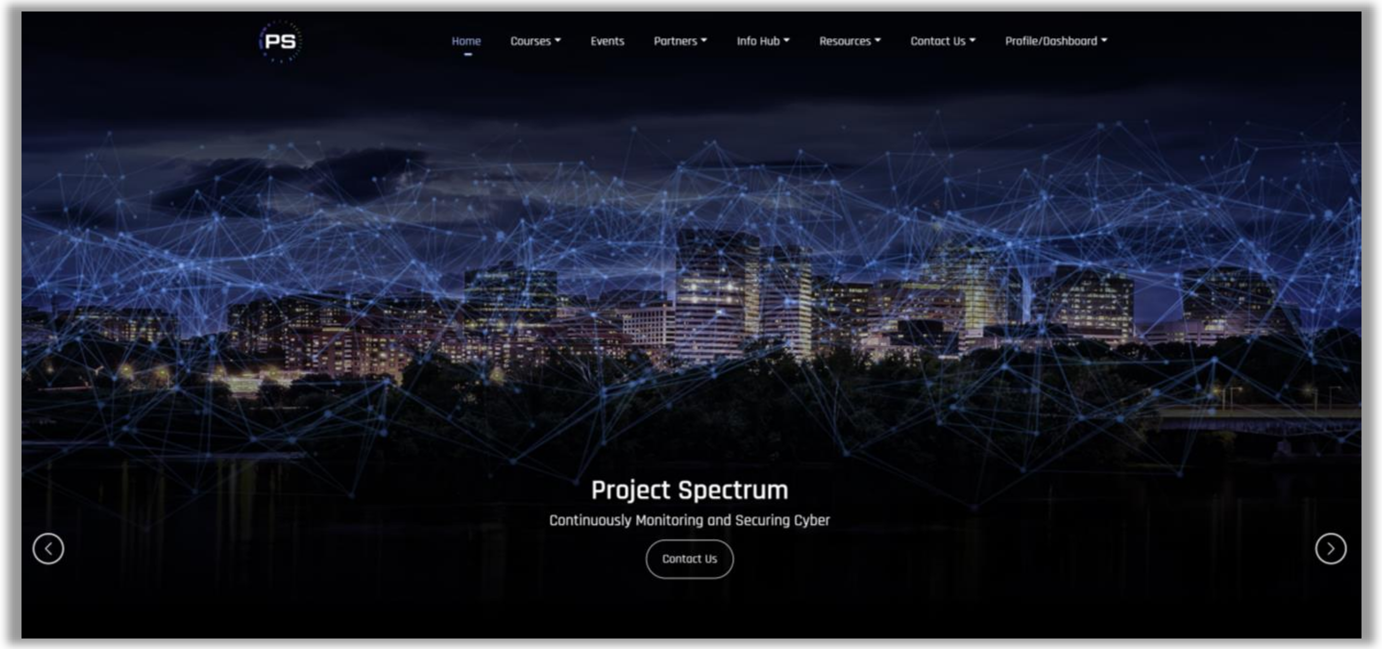
Detail View:
A3 COMPANY - (Return to Top)

	DFARS 252.204-7012 Compliance	Most Recent Assessment	Assessment Score	Confidence Level	Standard used to Assess	Assessing CAGE or DoDAAC	Assessment Scope	Included CAGEs/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	!AAA3 A3 COMPANY	06/16/2021	Company A3 SSP		06/16/2021	🗑
✎		05/11/2021	110	BASIC	NIST SP 800-171		ENCLAVE	!AAA4 A4 COMPANY	N/A	2021-469	1	05/10/2021	🗑

1 | 20 items per page | 1 - 2 of 2 items

Project Spectrum Resources

- Self-Assessment Toolkit
- Cyber Readiness Dashboard
- SPRS Score
- Remediation Plan Template



Project Spectrum

Continuously Monitoring and Securing Cyber

- Security System Plans (SSP) Template
- Plans of Action and Milestones (POA&M)
- APEX Counselor PowerPoint Presentation
- Project Spectrum Instructional Playbook
- Cyber Advisory Services
- Cybersecurity Training and Education
- Cybersecurity Blogs
- Cybersecurity Newsletters
- Project Spectrum Briefings

Connect With Project Spectrum

Training Webinars

projectspectrum.io

outreach@
projectspectrum.io

Social Media

- in Project Spectrum
- @Proj_Spectrum
- ▶ Project Spectrum

THANK YOU

FOR YOUR ATTENTION

PROJECT SPECTRUM