VIRTUAL

SMALL BUSINESS TRAINING WEEK 2021

SBTW21

BUILD ★ GROW ★ ELEVATE

Expanding the Defense Industrial Base

PROJECT SPECTRUM

Cybersecurity Resources

KAREEM SYKES

PROJECT SPECTRUM PROGRAM MANAGER

8/17/2021

UNCLASSIFIED

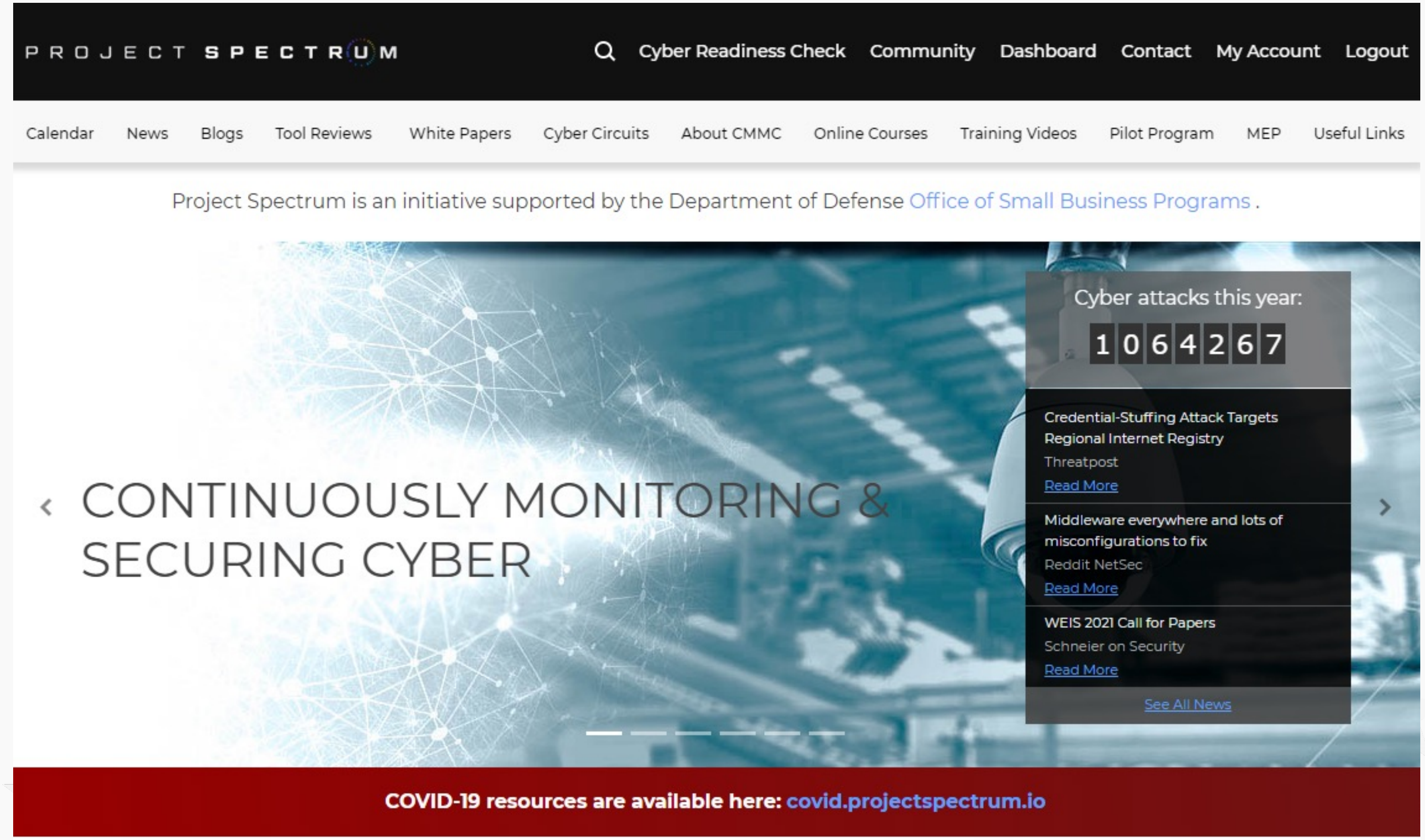
What is Project Spectrum?

Project Spectrum is a DoD-sponsored initiative that provides companies, institutions, and organizations with a comprehensive, cost-effective platform of cybersecurity information, resources, tools, and training. Our mission is to improve cybersecurity readiness, resiliency, and compliance of small/medium-sized businesses and the Defense Industrial Base (DIB) manufacturing supply chain through:

- Policy guidance
- A customized dashboard for monitoring cybersecurity progress
- Expert analysis and intelligence from senior cyber advisors
- Educational courses and materials
- Tool and platform reviews
- Customized cybersecurity compliance plans
- Cybersecurity Maturity Model Certification (CMMC) training

Project Spectrum

UNCLASSIFIED



PROJECT SPECTRUM

Cyber Readiness Check | Community | Dashboard | Contact | My Account | Logout

Calendar | News | Blogs | Tool Reviews | White Papers | Cyber Circuits | About CMMC | Online Courses | Training Videos | Pilot Program | MEP | Useful Links

Project Spectrum is an initiative supported by the Department of Defense Office of Small Business Programs .

CONTINUOUSLY MONITORING & SECURING CYBER

Cyber attacks this year:

1064267

Credential-Stuffing Attack Targets Regional Internet Registry
Threatpost
Read More

Middleware everywhere and lots of misconfigurations to fix
Reddit NetSec
Read More

WEIS 2021 Call for Papers
Schneier on Security
Read More

See All News

COVID-19 resources are available here: covid.projectspectrum.io

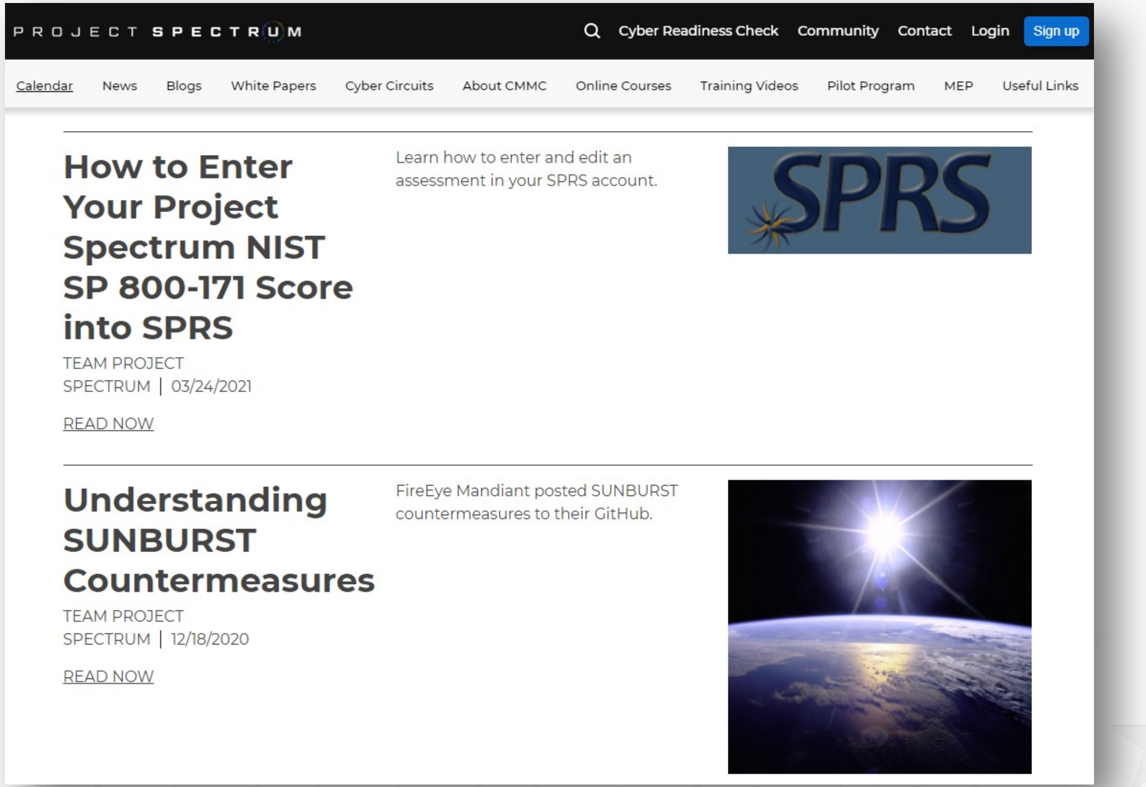
https://projectspectrum.io

Federal Policy Compliance

- Project Spectrum operates under the authority of the
  - **2019 National Defense Authorization Act (NDAA)**
    - Section 1644: Assistance for small manufacturers in the defense industrial supply chain and universities.
  - **2021 National Defense Authorization Act**
    - Section 1724: Responsibility for cybersecurity and critical infrastructure protection of the defense industrial base.
    - Section 1738: Assistance for small manufacturers in the defense industrial supply chain on matters relating to cybersecurity.
- We offer compliance with existing Defense Federal Acquisition Regulation Supplement (DFARS) regulations
  - 2019-D041 Interim Rule and its associated clauses (252.204-7008, 252.204-7012, 252.204-7019-21).
  - Regulations require compliance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 for the safeguarding of defense-relevant information and cyber incident reporting.

Policy Compliance

UNCLASSIFIED



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.

TEAM PROJECT SPECTRUM | 03/24/2021

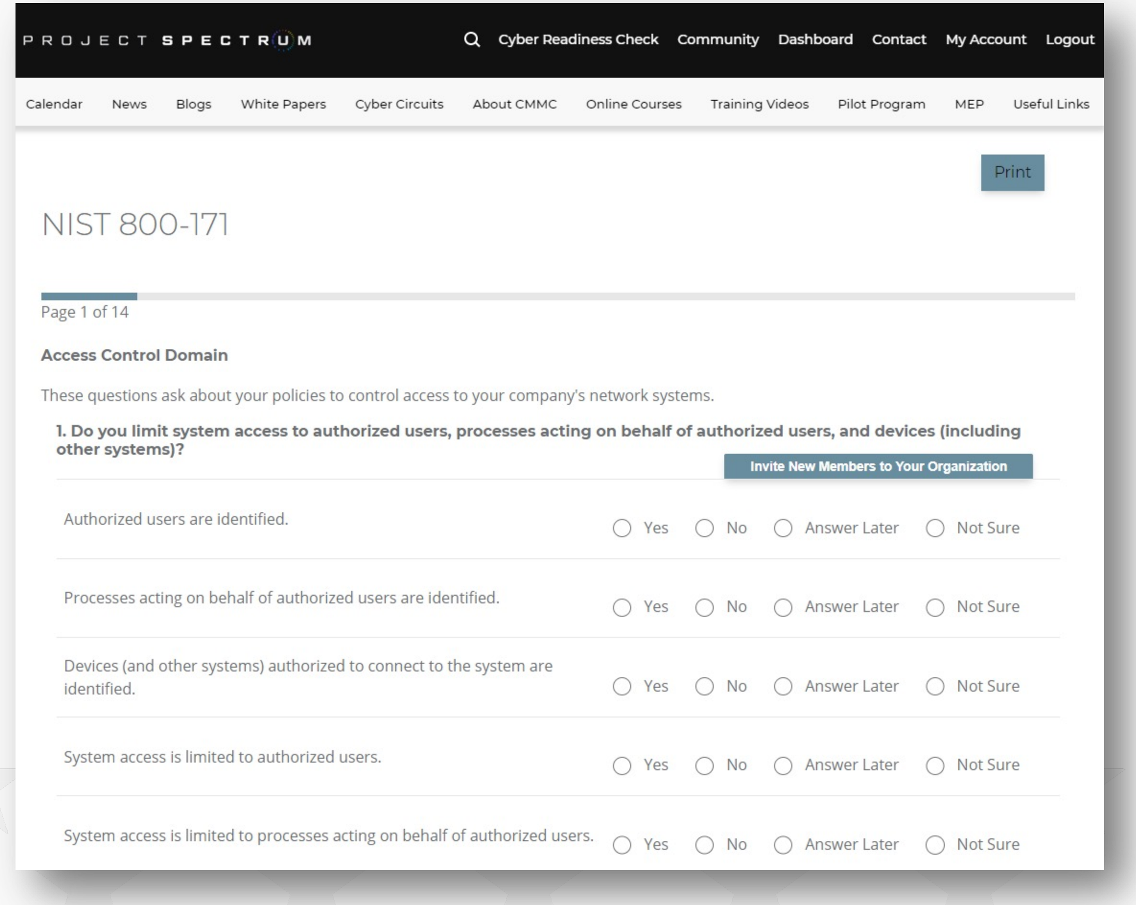
READ NOW

Understanding SUNBURST Countermeasures

FireEye Mandiant posted SUNBURST countermeasures to their GitHub.

TEAM PROJECT SPECTRUM | 12/18/2020

READ NOW



NIST 800-171

Page 1 of 14

Access Control Domain

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)?

Authorized users are identified. ○ Yes ○ No ○ Answer Later ○ Not Sure

Processes acting on behalf of authorized users are identified. ○ Yes ○ No ○ Answer Later ○ Not Sure

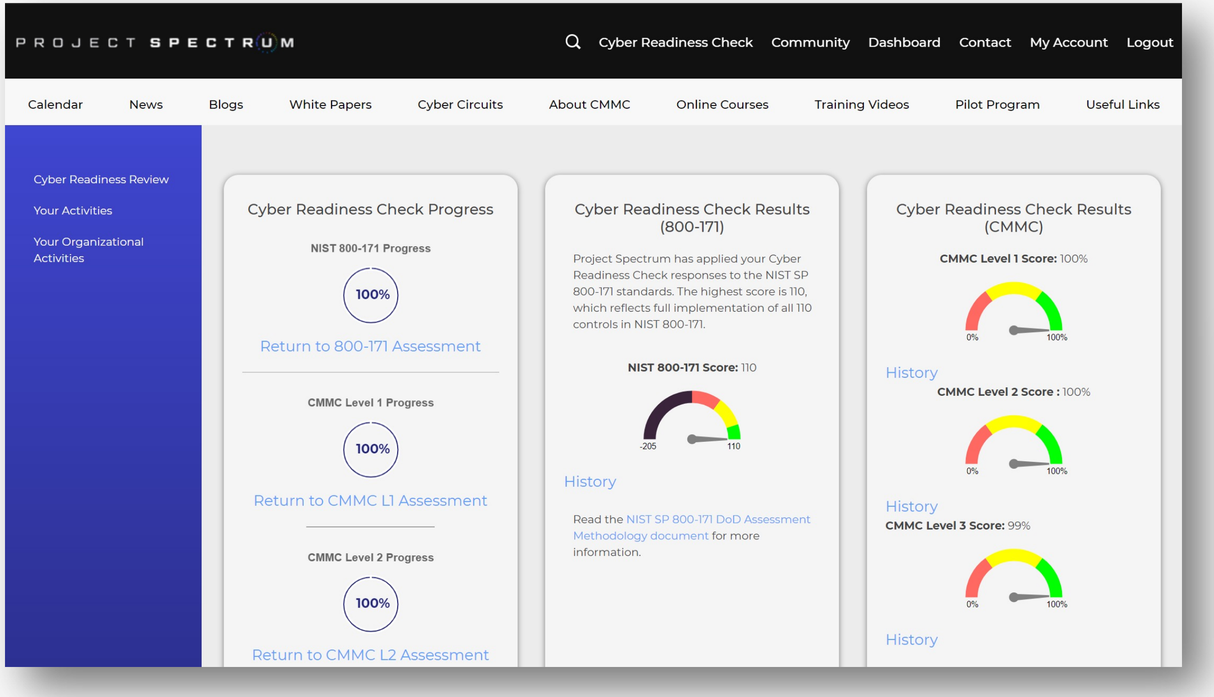
Devices (and other systems) authorized to connect to the system are identified. ○ Yes ○ No ○ Answer Later ○ Not Sure

System access is limited to authorized users. ○ Yes ○ No ○ Answer Later ○ Not Sure

System access is limited to processes acting on behalf of authorized users. ○ Yes ○ No ○ Answer Later ○ Not Sure

Customized Dashboard

UNCLASSIFIED



Cyber Readiness Check Progress

NIST 800-171 Progress

100%

Return to 800-171 Assessment

CMMC Level 1 Progress

100%

Return to CMMC L1 Assessment

CMMC Level 2 Progress

100%

Return to CMMC L2 Assessment

Cyber Readiness Check Results (800-171)

Project Spectrum has applied your Cyber Readiness Check responses to the NIST SP 800-171 standards. The highest score is 110, which reflects full implementation of all 110 controls in NIST 800-171.

NIST 800-171 Score: 110

History

Read the NIST SP 800-171 DoD Assessment Methodology document for more information.

Cyber Readiness Check Results (CMMC)

CMMC Level 1 Score: 100%

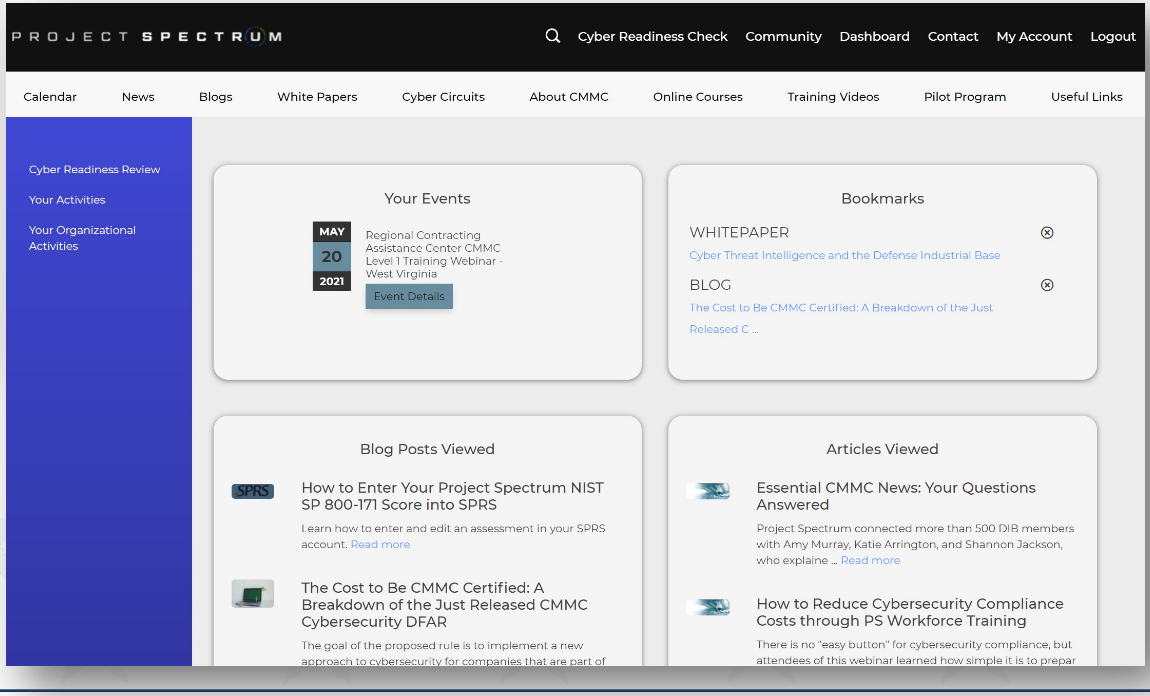
History

CMMC Level 2 Score : 100%

History

CMMC Level 3 Score: 99%

History



Your Events

MAY 20 2021

Regional Contracting Assistance Center CMMC Level 1 Training Webinar - West Virginia

Event Details

Bookmarks

WHITEPAPER ⊗

Cyber Threat Intelligence and the Defense Industrial Base

BLOG ⊗

The Cost to Be CMMC Certified: A Breakdown of the Just Released C ...

Blog Posts Viewed

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. Read more

The Cost to Be CMMC Certified: A Breakdown of the Just Released CMMC Cybersecurity DFAR

The goal of the proposed rule is to implement a new approach to cybersecurity for companies that are part of

Articles Viewed

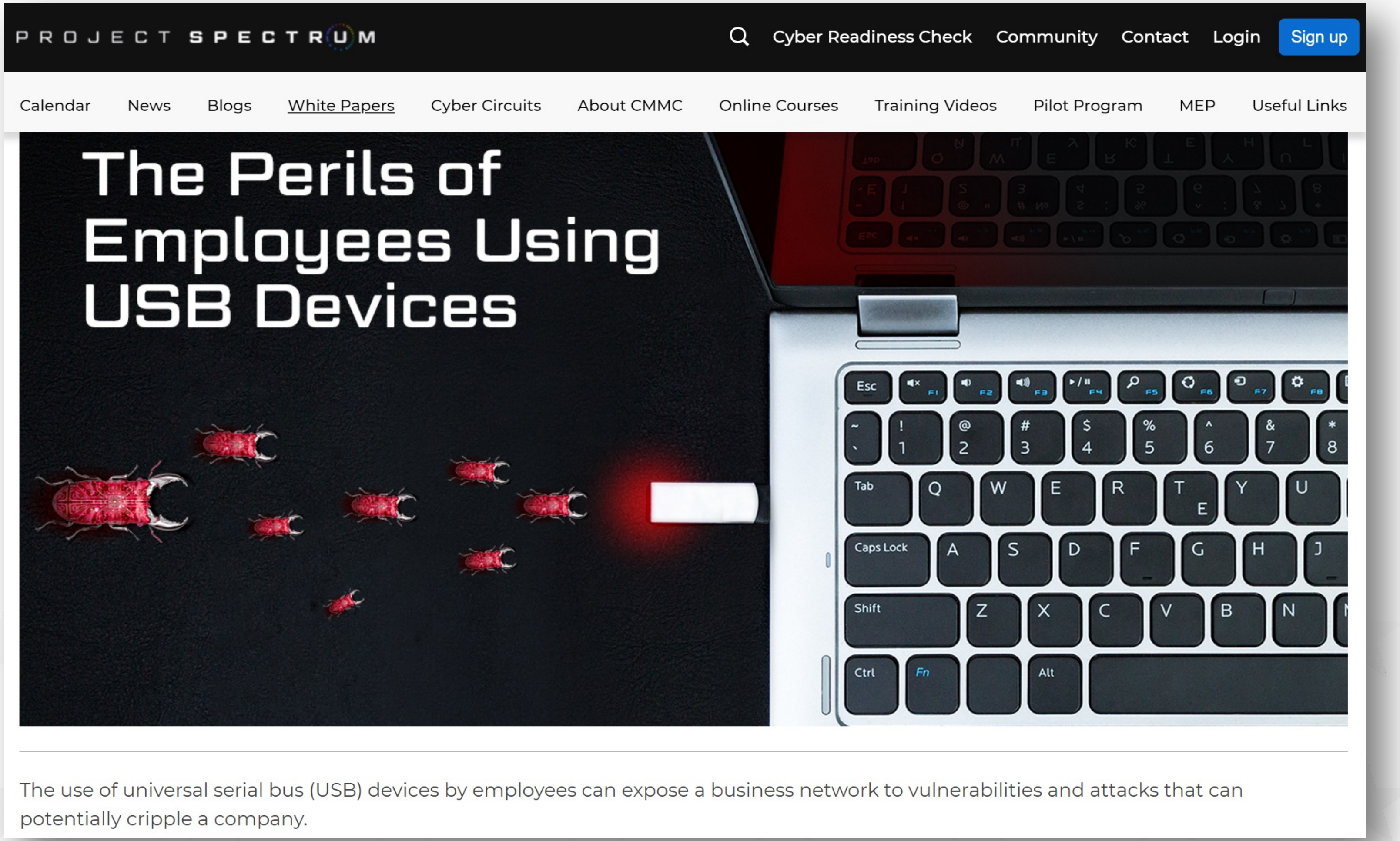
Essential CMMC News: Your Questions Answered

Project Spectrum connected more than 500 DIB members with Amy Murray, Katie Arrington, and Shannon Jackson, who explaine ... Read more

How to Reduce Cybersecurity Compliance Costs through PS Workforce Training

There is no "easy button" for cybersecurity compliance, but attendees of this webinar learned how simple it is to prepar

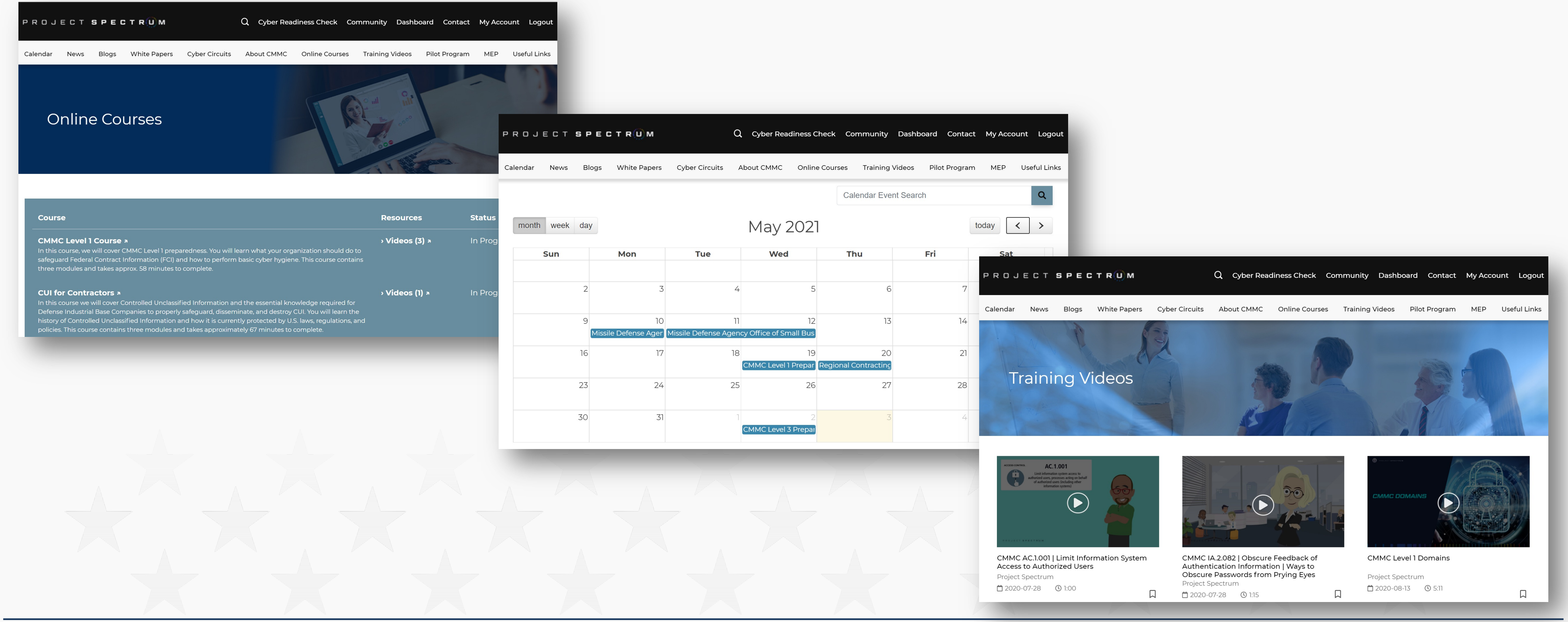
Analysis and Intelligence from our Cyber Advisors



The Perils of Employees Using USB Devices

The use of universal serial bus (USB) devices by employees can expose a business network to vulnerabilities and attacks that can potentially cripple a company.

Educational Resources



Online Courses

Course	Resources	Status
CMMC Level 1 Course ↗ In this course, we will cover CMMC Level 1 preparedness. You will learn what your organization should do to safeguard Federal Contract Information (FCI) and how to perform basic cyber hygiene. This course contains three modules and takes approx. 58 minutes to complete.	› Videos (3) ↗	In Prog
CUI for Contractors ↗ In this course we will cover Controlled Unclassified Information and the essential knowledge required for Defense Industrial Base Companies to properly safeguard, disseminate, and destroy CUI. You will learn the history of Controlled Unclassified Information and how it is currently protected by U.S. laws, regulations, and policies. This course contains three modules and takes approximately 67 minutes to complete.	› Videos (1) ↗	In Prog

May 2021

Sun	Mon	Tue	Wed	Thu	Fri	Sat
2	3	4	5	6	7	
9	10 Missile Defense Ager	11 Missile Defense Agency Office of Small Bus	12	13	14	
16	17	18	19 CMMC Level 1 Prepar	20 Regional Contracting	21	
23	24	25	26	27	28	
30	31	1	2 CMMC Level 3 Prepar	3	4	

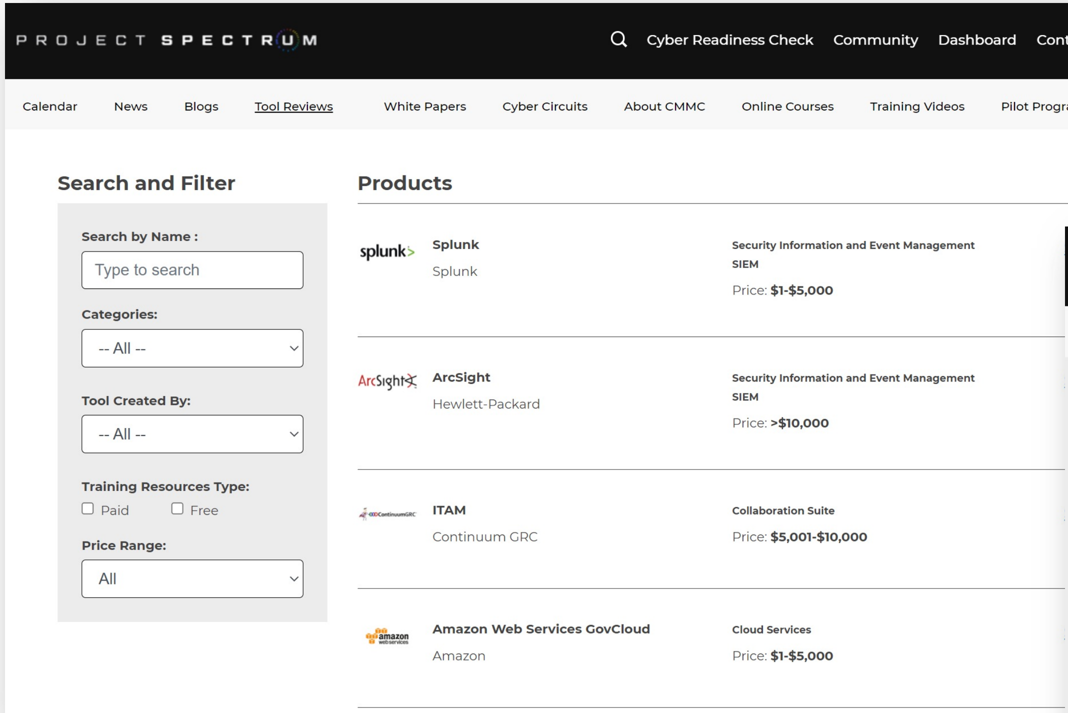
Training Videos

CMMC AC.1.001 | Limit Information System Access to Authorized Users
Project Spectrum
2020-07-28 1:00

CMMC IA.2.082 | Obscure Feedback of Authentication Information | Ways to Obscure Passwords from Prying Eyes
Project Spectrum
2020-07-28 1:15

CMMC Level 1 Domains
Project Spectrum
2020-08-13 5:11

Tool Review



Search and Filter

Search by Name : Type to search

Categories: -- All --

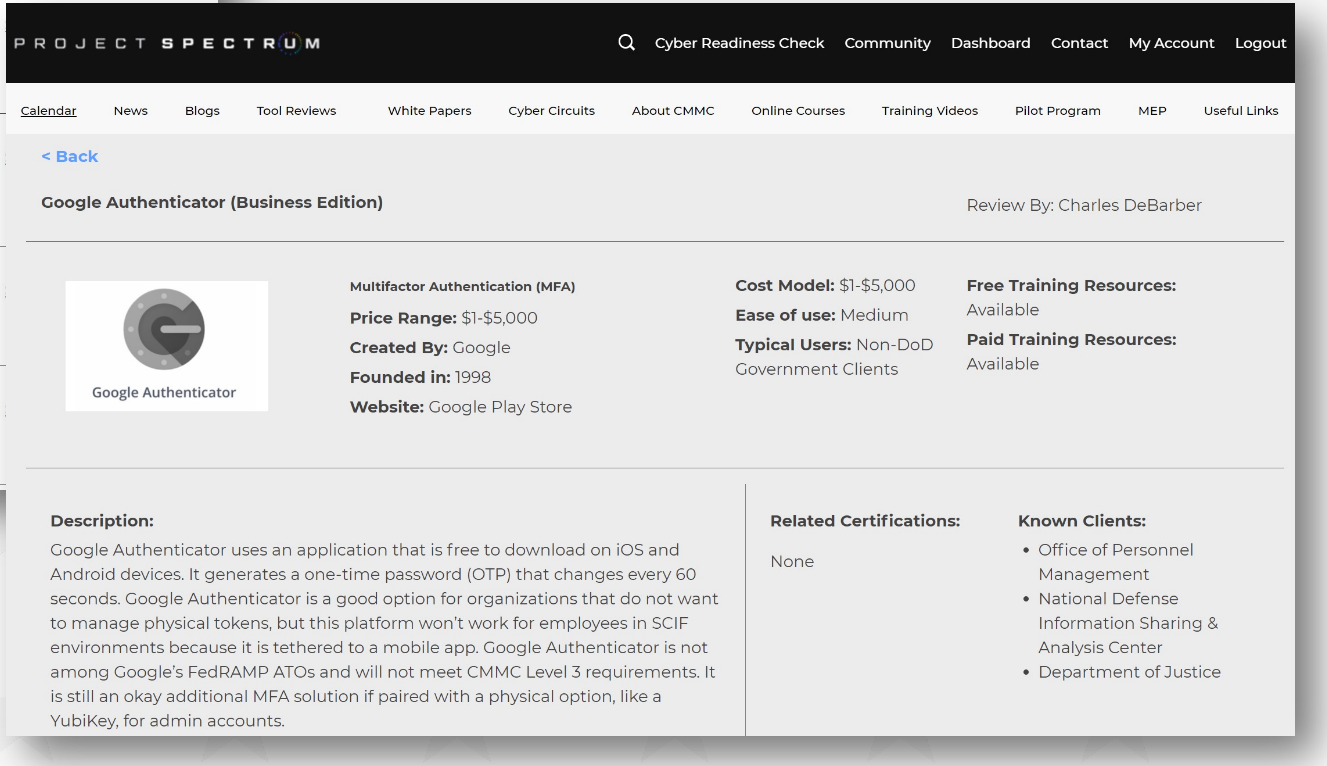
Tool Created By: -- All --

Training Resources Type: □ Paid □ Free

Price Range: All

Products

Splunk Splunk	Security Information and Event Management SIEM Price: **$1-$5,000**
ArcSight Hewlett-Packard	Security Information and Event Management SIEM Price: **>$10,000**
ITAM Continuum GRC	Collaboration Suite Price: **$5,001-$10,000**
Amazon Web Services GovCloud Amazon	Cloud Services Price: **$1-$5,000**



Google Authenticator (Business Edition)

Review By: Charles DeBarber

Multifactor Authentication (MFA)

Price Range: $1-$5,000
Created By: Google
Founded in: 1998
Website: Google Play Store

Cost Model: $1-$5,000
Ease of use: Medium
Typical Users: Non-DoD Government Clients

Free Training Resources: Available
Paid Training Resources: Available

Description:

Google Authenticator uses an application that is free to download on iOS and Android devices. It generates a one-time password (OTP) that changes every 60 seconds. Google Authenticator is a good option for organizations that do not want to manage physical tokens, but this platform won't work for employees in SCIF environments because it is tethered to a mobile app. Google Authenticator is not among Google's FedRAMP ATOs and will not meet CMMC Level 3 requirements. It is still an okay additional MFA solution if paired with a physical option, like a YubiKey, for admin accounts.

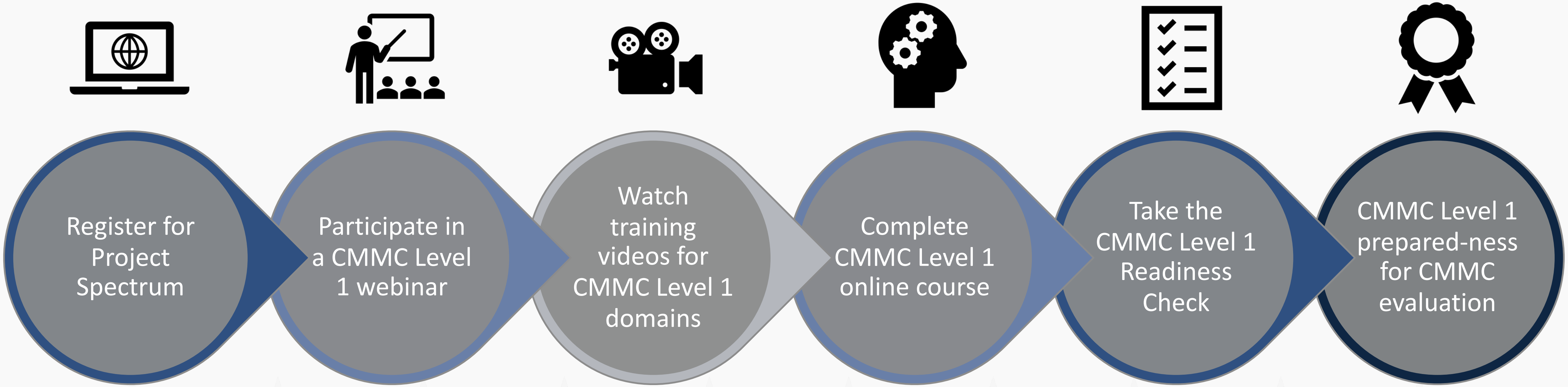
Related Certifications:

None

Known Clients:

- Office of Personnel Management
- National Defense Information Sharing & Analysis Center
- Department of Justice

Journey to CMMC Level 1 Compliance



Register for Project Spectrum

Participate in a CMMC Level 1 webinar

Watch training videos for CMMC Level 1 domains

Complete CMMC Level 1 online course

Take the CMMC Level 1 Readiness Check

CMMC Level 1 prepared-ness for CMMC evaluation

Project Spectrum Collaborations

Mentor Protégé Program

- The U.S. Department of Defense (DoD) Mentor-Protégé Program (MPP) helps small businesses (Protégés) successfully compete for contract awards by partnering with large companies (Mentors) under individual, project-based agreements lasting two years or less.
- Mentor-Protégé Agreements (MPAs) provide business infrastructure developmental assistance and technology transfer.
  - Examples of developmental assistance include human resources training, business development initiatives, capture management and proposal development training, or DCAA-compliant accounting system implementation training.
  - Technology transfer can include implementation of specific technology that will provide a benefit to a DoD program, such as quality management systems or certifications.

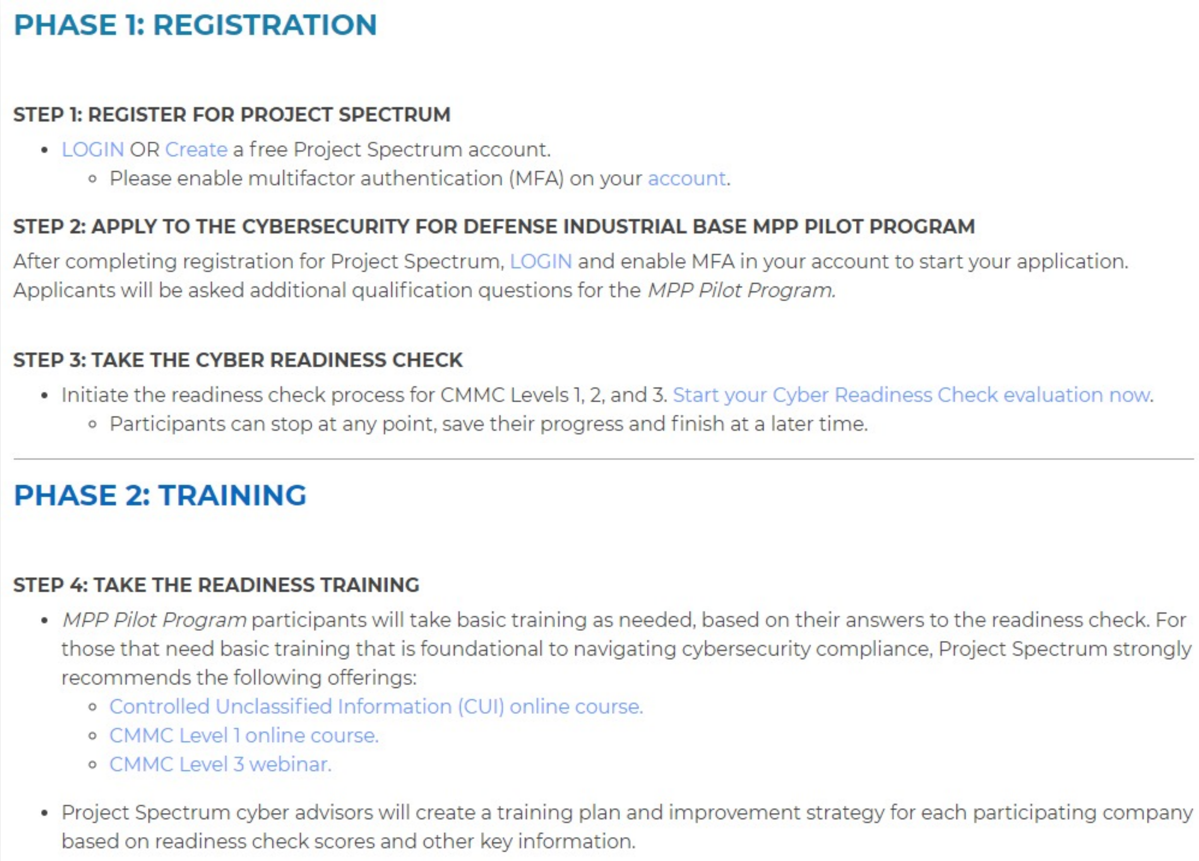
Manufacturing Extension Partnership

- We are working together to provide small-to-medium-sized manufacturers with a self-directed platform for cutting-edge cybersecurity compliance training, tools, and other resources.

MPP Cybersecurity Pilot Program Objectives

- Enroll MPP participants and other select companies.
  - Target the Research and Development, Manufacturing, and Knowledge-based Service sectors.
  - Accept companies that possess the necessary resources to respond to vulnerabilities identified by the program.
- The Pilot Program will:
  - Increase MPP participants’ compliance and cyber incident reporting.
  - Foster measurable increases in cyber hygiene, compliance, and incident reporting.
  - Provide exclusive educational materials, tools, and advisory services.

Cybersecurity for Defense Industrial Base MPP Pilot Program



PHASE 1: REGISTRATION

STEP 1: REGISTER FOR PROJECT SPECTRUM

- LOGIN OR Create a free Project Spectrum account.
    - Please enable multifactor authentication (MFA) on your account.

STEP 2: APPLY TO THE CYBERSECURITY FOR DEFENSE INDUSTRIAL BASE MPP PILOT PROGRAM

After completing registration for Project Spectrum, LOGIN and enable MFA in your account to start your application. Applicants will be asked additional qualification questions for the *MPP Pilot Program*.

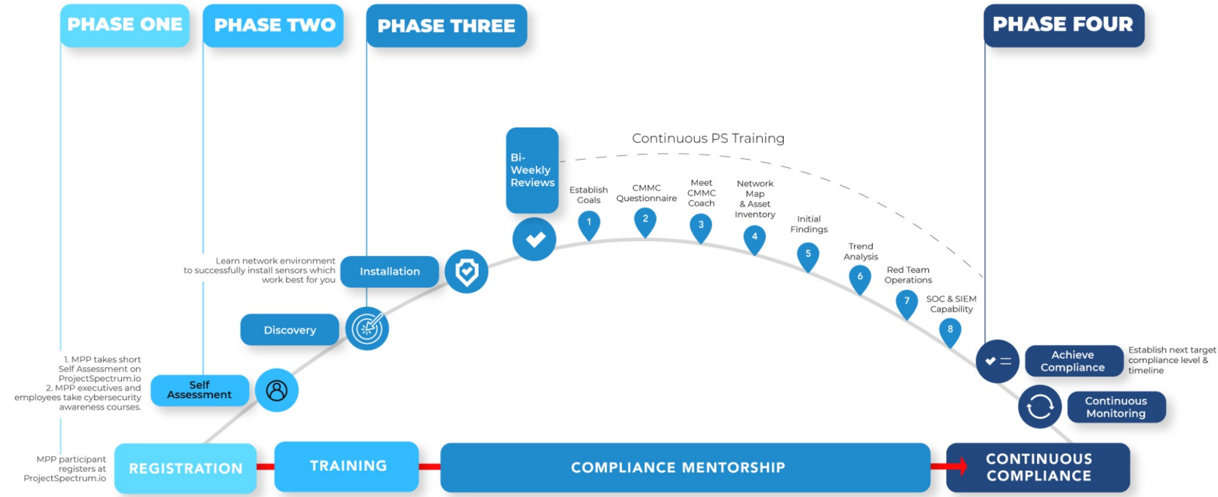
STEP 3: TAKE THE CYBER READINESS CHECK

- Initiate the readiness check process for CMMC Levels 1, 2, and 3. Start your Cyber Readiness Check evaluation now.
    - Participants can stop at any point, save their progress and finish at a later time.

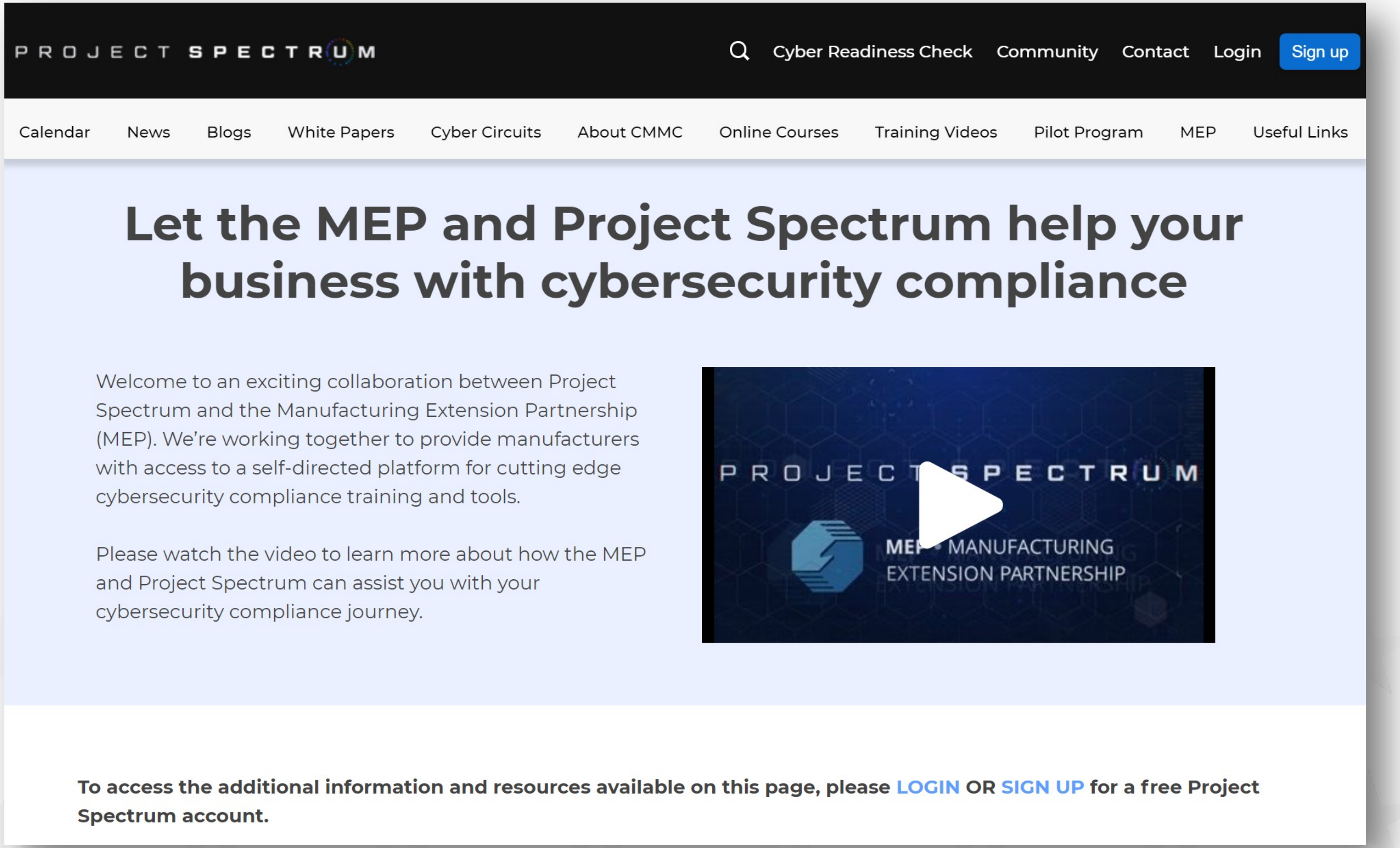
PHASE 2: TRAINING

STEP 4: TAKE THE READINESS TRAINING

- *MPP Pilot Program* participants will take basic training as needed, based on their answers to the readiness check. For those that need basic training that is foundational to navigating cybersecurity compliance, Project Spectrum strongly recommends the following offerings:
    - Controlled Unclassified Information (CUI) online course.
    - CMMC Level 1 online course.
    - CMMC Level 3 webinar.
- Project Spectrum cyber advisors will create a training plan and improvement strategy for each participating company based on readiness check scores and other key information.



Manufacturing Extension Partnership



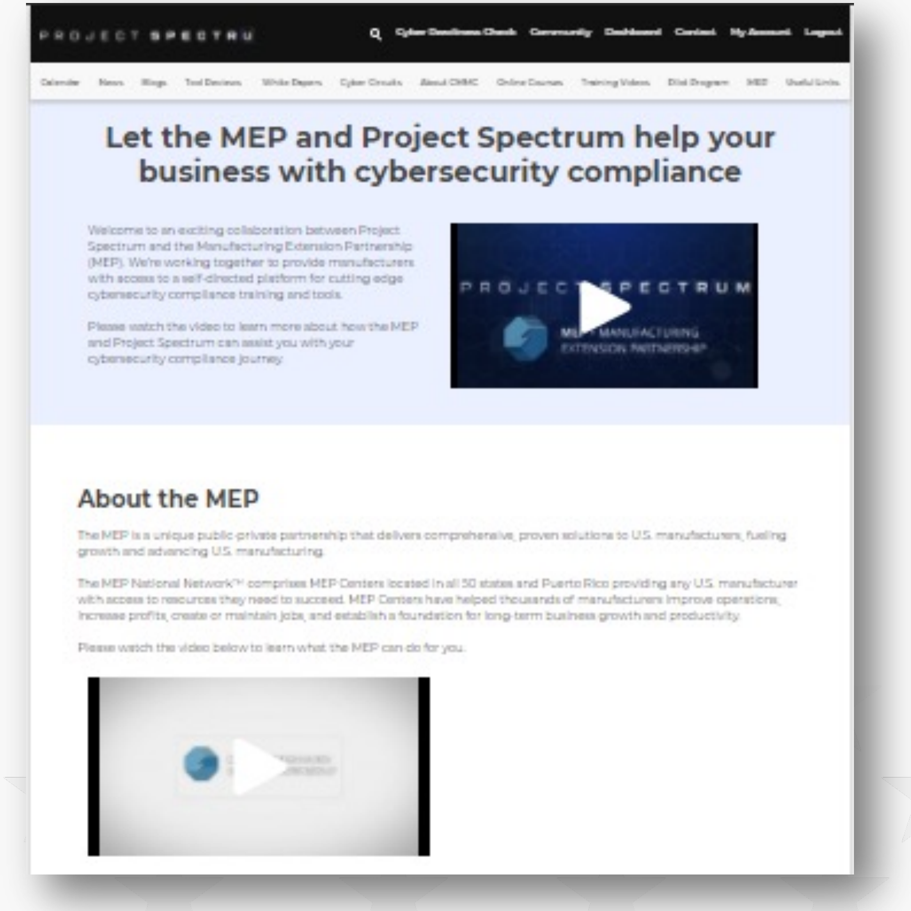
Let the MEP and Project Spectrum help your business with cybersecurity compliance

Welcome to an exciting collaboration between Project Spectrum and the Manufacturing Extension Partnership (MEP). We're working together to provide manufacturers with access to a self-directed platform for cutting edge cybersecurity compliance training and tools.

Please watch the video to learn more about how the MEP and Project Spectrum can assist you with your cybersecurity compliance journey.

To access the additional information and resources available on this page, please LOGIN OR SIGN UP for a free Project Spectrum account.

Manufacturing Extension Partnership



Let the MEP and Project Spectrum help your business with cybersecurity compliance

Welcome to an exciting collaboration between Project Spectrum and the Manufacturing Extension Partnership (MEP). We're working together to provide manufacturers with access to a self-directed platform for cutting edge cybersecurity compliance training and tools.

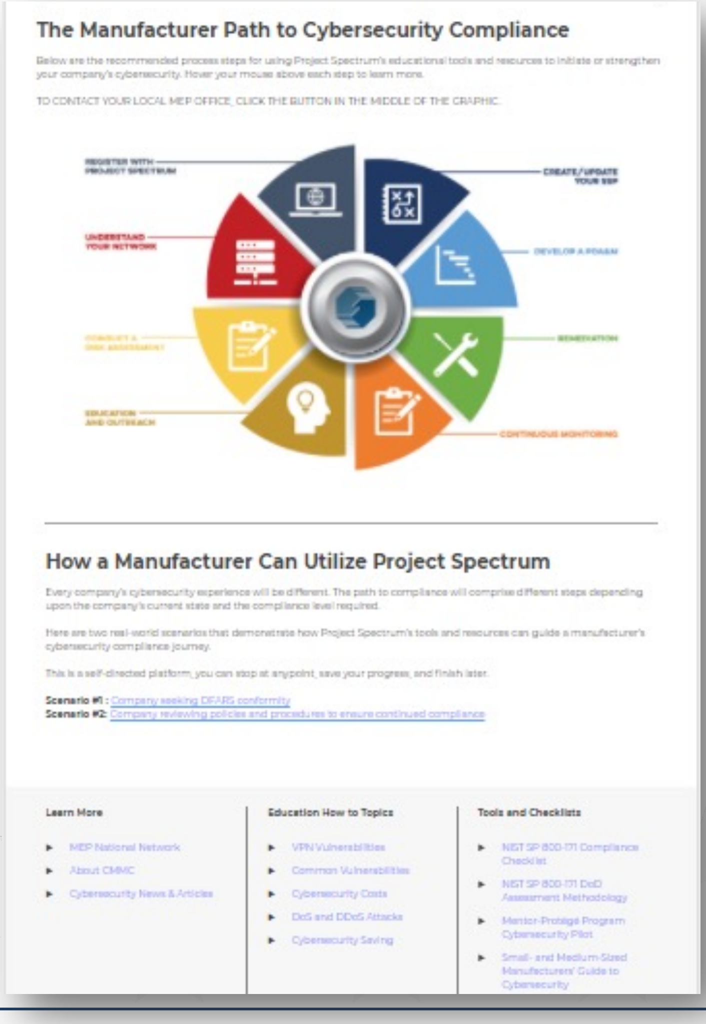
Please watch the video to learn more about how the MEP and Project Spectrum can assist you with your cybersecurity compliance journey.

About the MEP

The MEP is a unique public-private partnership that delivers comprehensive, proven solutions to U.S. manufacturers, fueling growth and advancing U.S. manufacturing.

The MEP National Network™ comprises MEP Centers located in all 50 states and Puerto Rico providing any U.S. manufacturer with access to resources they need to succeed. MEP Centers have helped thousands of manufacturers improve operations, increase profits, create or maintain jobs, and establish a foundation for long-term business growth and productivity.

Please watch the video below to learn what the MEP can do for you.



The Manufacturer Path to Cybersecurity Compliance

Below are the recommended process steps for using Project Spectrum's educational tools and resources to initiate or strengthen your company's cybersecurity. Hover your mouse above each step to learn more.

TO CONTACT YOUR LOCAL MEP OFFICE, CLICK THE BUTTON IN THE MIDDLE OF THE GRAPHIC.

How a Manufacturer Can Utilize Project Spectrum

Every company's cybersecurity experience will be different. The path to compliance will comprise different steps depending upon the company's current state and the compliance level required.

Here are two real-world scenarios that demonstrate how Project Spectrum's tools and resources can guide a manufacturer's cybersecurity compliance journey.

This is a self-directed platform, you can stop at anypoint, save your progress, and finish later.

Scenario #1 : Company seeking DFARS conformity
Scenario #2: Company reviewing policies and procedures to ensure continued compliance

Learn More

- MEP National Network
- About CMMC
- Cybersecurity News & Articles

Education How to Topics

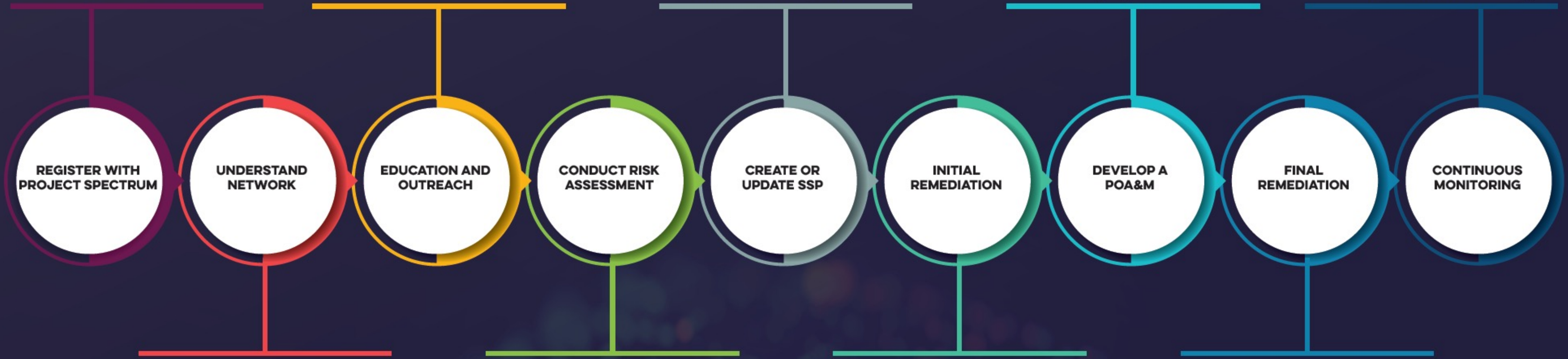
- VPN Vulnerabilities
- Common Vulnerabilities
- Cybersecurity Costs
- DoS and DDoS Attacks
- Cybersecurity Saving

Tools and Checklists

- NIST SP 800-171 Compliance Checklist
- NIST SP 800-171 DoD Assessment Methodology
- Mentor-Protégé Program Cybersecurity Pilot
- Small- and Medium-Sized Manufacturers' Guide to Cybersecurity

MANUFACTURER SCENARIO #1

Eagle Defense Manufacturing (EDM) is seeking DFARS 7012 conformity. The company may seek CMMC Level 3 certification in the future.



REGISTER WITH PROJECT SPECTRUM

EDM registers with Project Spectrum and gets access to technical/policy information, self-assessments, and a personalized dashboard to track conformity journey progress.

UNDERSTAND NETWORK

EDM reviews policies, network maps, and controls to better understand the current state; determines the required certification level(s); and accesses training courses, webinars, and white papers to gain knowledge.

EDUCATION AND OUTREACH

EEDM utilizes the SSP Fundamentals course and begins drafting its first SSP addressing all conformity requirements identified through the self-assessments.

CONDUCT RISK ASSESSMENT

EDM accesses and completes self-assessments for CMMC Levels 1-3 to confirm the current conformity levels. EDM gets written guidance for uploading the results to SPRS.

CREATE OR UPDATE SSP

EDM uses Project Spectrum resources (videos and forum posts) to create an SSP that addresses each control/practice that needs remediation.

INITIAL REMEDIATION

EDM takes initial remediation steps based on interim findings to determine if vulnerabilities can be fixed quickly.

DEVELOP A POA&M

EDM finishes initial remediation and develops a POA&M to track vulnerabilities and determine a timeline for conformity. The company uses the PS dashboard and readiness checks to track progress.

FINAL REMEDIATION

EDM takes the steps determined by the POA&M to address CUI storage and lack of multifactor authentication (MFA). The company utilizes PS videos and training courses to develop a conformity solution.

CONTINUOUS MONITORING

EDM monitors and periodically checks up on the SSP, which is a "living document." The company continues to access and utilize PS analysis and information about critical vulnerabilities and transformation technologies.

PROJECT SPECTRUM

MEP • MANUFACTURING EXTENSION PARTNERSHIP

Small Business Support

Procurement Technical Assistance Centers (PTACs)

- Collaborated with 49 PTACs – 1,900+ attendees
- Spoke at APTAC conferences

CMMC Preparedness Training

- Level 1 & Level 3 webinars – 3,000+ attendees
- Level 1 online course – 500+ participants

Training Videos

- Videos are posted to projectspectrum.io and YouTube
- VOLTS | Cybersecurity Tips – 9,000+ views

Cyber Circuits

- 13 events – 2,100+ attendees
- Speakers from the Office of the Secretary of Defense, Cybersecurity Maturity Model Certification – Accreditation Body, and U.S. Small Business Administration

Connect with Us

EMAIL
outreach@
projectspectrum.io

MENTOR PROTÉGÉ PILOT PROGRAM

MONTHLY WEBINARS

SOCIAL MEDIA

project spectrum.io

VIRTUAL

SMALL BUSINESS TRAINING WEEK 2021

SBTW21

BUILD ★ GROW ★ ELEVATE

Expanding the Defense Industrial Base

Thank you

Kareem Sykes
Program Manager, Project Spectrum
www.projectspectrum.io
outreach@projectspectrum.io