PROJECT SPECTRUM

Supporting Resilience in Cybersecurity and Developing the DIB Cloud Environment

Derrick Davis

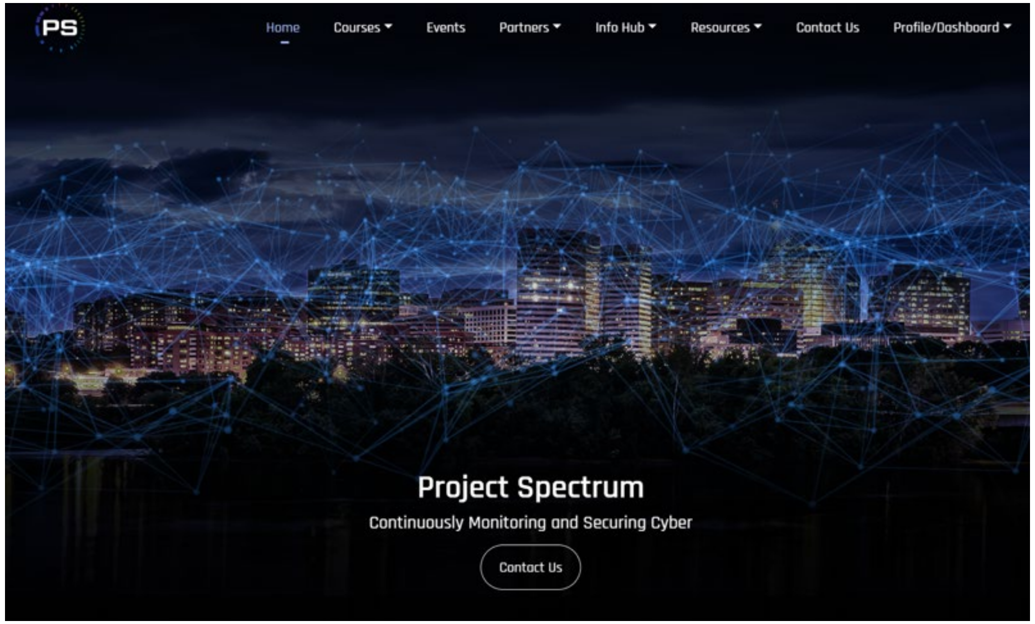
1/29/2024

CYBERSECURITY FOR SMALL BUSINESSES AND THE DIB

- Project Spectrum is a DoD-supported initiative through the Office of Small Business Programs (OSBP)

- PS provides a comprehensive, cost-effective platform of cybersecurity information, resources, tools, and training

- The PS mission is to improve the cybersecurity readiness, resilience, and compliance of small/medium-sized businesses and all DIB companies



Project Spectrum

Continuously Monitoring and Securing Cyber

Why Project Spectrum?

- Small businesses comprise more than 70% of the DIB
- 25% of DoD prime contracts are awarded to small businesses
- Nearly 43% of all cyberattacks target small- and medium-sized businesses

(Statistics as of August 2023)

The numbers definitively show that small businesses within the DIB are the most targeted. Project Spectrum’s no-cost security services help level the playing field.

WHY SMALL BUSINESSES ARE TARGETED

Access to sensitive government information

Intellectual property

Connection with larger defense contractors

Focused on production and meeting deadlines, not ‘extraneous’ activities like cybersecurity

Limited cybersecurity resources due to funding; ill-prepared to handle cyberattacks

The Government 'Mandate'

Via FAR's clauses 252.204-21 and 252.204-7012, the Federal Government requires businesses to properly protect both Federal Contract Information (FCI) and Controlled Unclassified Information (CUI).

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.

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

Examples of FCI

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

Examples of CUI

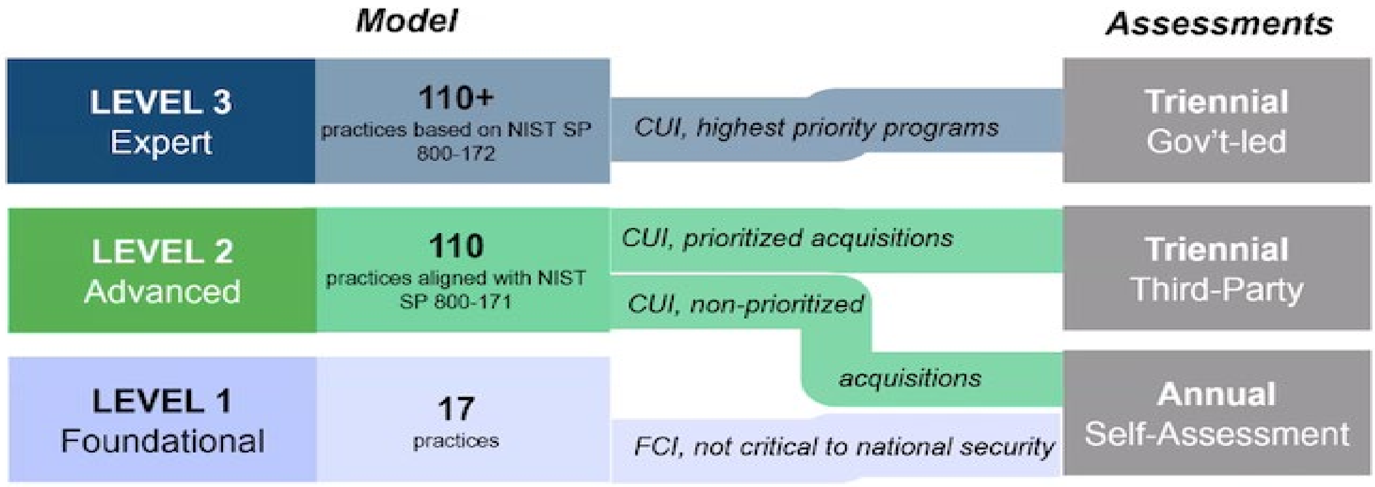
- Proprietary Business Information (PBI)
- Unclassified Controlled Technical Information (UCTI)
- Sensitive but Unclassified (SBU)
- For Official Use Only (FOUO)
- Law Enforcement Sensitive (LES)

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 carries the highest priority for DoD programs.

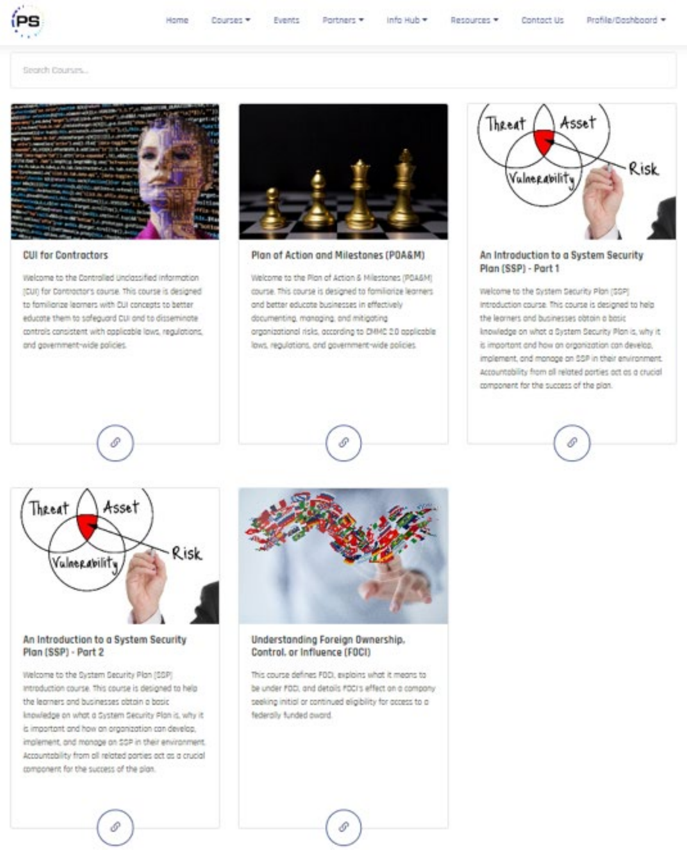


Model			Assessments
LEVEL 3 Expert	110+ practices based on NIST SP 800-172	CUI, highest priority programs	Triennial Gov’t-led
LEVEL 2 Advanced	110 practices aligned with NIST SP 800-171	CUI, prioritized acquisitions	Triennial Third-Party
		CUI, non-prioritized acquisitions	Annual Self-Assessment
LEVEL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

CYBERSECURITY TRAINING AND RESOURCES

Project Spectrum has developed a robust cybersecurity training program built upon a proprietary Learning Management System:

- 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



CUI for Contractors

Welcome to the Controlled Unclassified Information (CUI) for Contractor's course. This course is designed to familiarize learners with CUI concepts to better educate them to safeguard CUI and to disseminate controls consistent with applicable laws, regulations, and government-wide policies.

Plan of Action and Milestones (POA&M)

Welcome to the Plan of Action & Milestones (POA&M) course. This course is designed to familiarize learners and better educate businesses in effectively documenting, managing, and mitigating organizational risks, according to CMMC 2.0 applicable laws, regulations, and government-wide policies.

An Introduction to a System Security Plan (SSP) - Part 1

Welcome to the System Security Plan (SSP) introduction course. This course is designed to help the learners and businesses obtain a basic knowledge on what a System Security Plan is, why it is important and how an organization can develop, implement, and manage an SSP in their environment. Accountability from all related parties act as a crucial component for the success of the plan.

An Introduction to a System Security Plan (SSP) - Part 2

Welcome to the System Security Plan (SSP) introduction course. This course is designed to help the learners and businesses obtain a basic knowledge on what a System Security Plan is, why it is important and how an organization can develop, implement, and manage an SSP in their environment. Accountability from all related parties act as a crucial component for the success of the plan.

Understanding Foreign Ownership, Control, or Influence (FOCI)

This course defines FOCI, explains what it means to be under FOCI, and details FOCI's effect on a company seeking initial or continued eligibility for access to a federally funded award.

Developing the DIB’s Secure Cloud Environment

Project Spectrum is leading the way in developing the DIB’s Secure Cloud Environment to ensure the protection of the DIB’s cyber-based assets.

Why do we need a Secure Cloud Environment for the DIB?

- Small businesses in the DIB are limited in their ability to meet increasing cybersecurity requirements for the protection of Department of Defense (DoD) information and operations.
- The problem is especially critical for small disadvantaged businesses that do not have the expertise or resources to meet the stringent DoD security controls along with emerging monitoring and mitigation requirements.
- A solution that only stores DoD data in such a secure, managed cloud does not need to meet the DoD requirements for on-premise security and safe storage and development of DoD technical data.

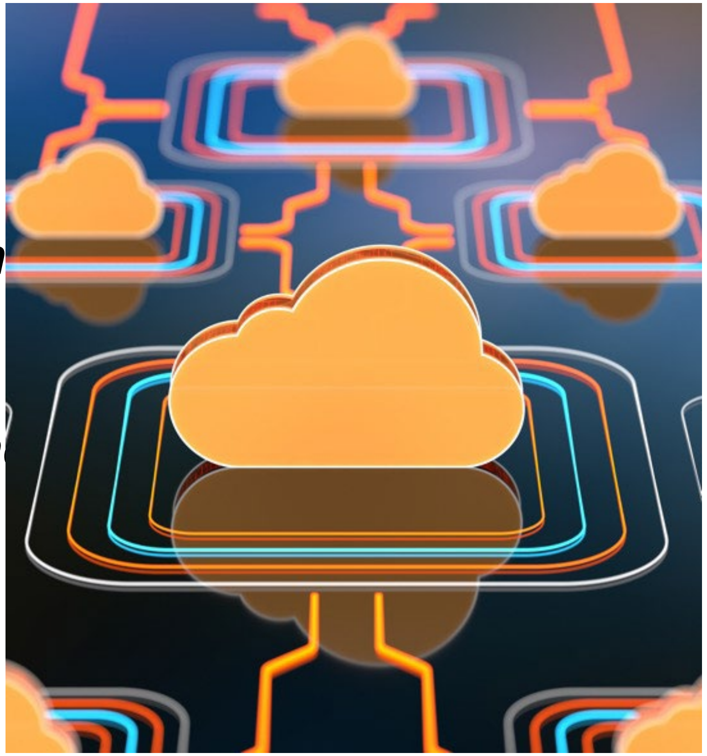
Secure Cloud Deployment Expectations

- We will provide a secure hosting environment that supports thin-client services to enable small business DIB companies to meet most DoD cybersecurity and emerging FOCI requirements as defined by statute.
- Our cloud architecture provides secure storage, processing, and transmission of controlled unclassified information through a virtual desktop technology.
- The solution supports CMMC / NIST 800-171 compliance and due diligence standards.
- The solution is cloud-agnostic and can be deployed on local servers (for OCONUS-based companies) and commercial cloud offerings such as AWS (for CONUS-based companies).
- The solution uses Infrastructure-as-Code for automated easy deployment.
- The solution provides secure clean-up when the environment is not used.

The Secure Cloud Environment Pilot Mechanics

Our DIB pilot will include 50 small businesses. As part of the pilot, we will collect the following metrics for evaluation:

- ***Usability of the platform (subjective metrics on ease of use)***
- ***System Performance metrics (including latency of access, uptim the infrastructure)***
- ***Compliance metrics (including number of reported incidents an number of cyber-attacks on the infrastructure)***
- ***Cost incurred per small business for using the infrastructure***
- ***Tool requirements per participating small business***



Deployment Timelines and Challenges

- The Secure Cloud Environment will be ready for pilot deployment and testing in the next six months on a cohort of 50 small businesses chosen from Mentor-Protégé Program and rapid innovation fund participants that are part of project Spectrum.

- The small businesses in the pilot cohort will be uniformly chosen from the OCONUS and CONUS-based companies.

- The usability and security will be assessed using the deployment.

- Cost estimate for the pilot will be approximately $10M.
  - *The government will cover the cost of the pilot at not cost to the participants. At scale, there will be a low-cost offering covered by the government and a subscription-based model paid for by users.*

- Challenges
  - *Liability associated with data storage belongs to pilot participants.*
  - *Ongoing cost to deploy and scale the secure cloud to CMMC level 2.0 companies*

HOW TO CONNECT WITH PROJECT SPECTRUM

- Visit https://projectspectrum.io and register for your FREE account
  - Begin your self-assessment to establish your baseline
  - Access the PS comprehensive suite of tools, training, and resources

- Email the PS Outreach and Cyber Advisory teams
  - Contact outreach@projectspectrum.io

- Follow PS on social media
  - LinkedIn, Twitter, and YouTube

- Check the PS calendar of events on our website for upcoming presentations, webinars, etc.

Q&A

PROJECT SPECTRUM

Thank you for your time and attention

Project Spectrum Briefing