PROJECT SPECTRUM

CYBERSECURITY FOR SMALL BUSINESS

Small Business Week 2023

June 21, 2023

Mr. Kareem Sykes
Program Manager,
Industry Engagement

CURRENT CYBER THREAT LANDSCAPE

Small businesses currently comprise **73% of the Defense Industrial Base** and have 25% of DoD prime contracts.

Nearly 43% of all cyberattacks target small- and medium-sized businesses, meaning they need to increase their vigilance.

The cost of a cyber attack **can be crippling:**

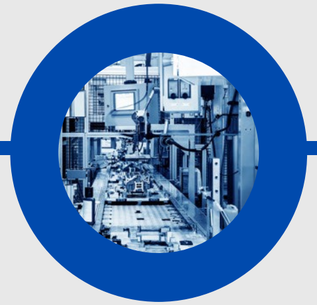
- Businesses must deal with compromised critical infrastructure, intellectual property theft, economic damage, geopolitical consequences, and a compromise of our national security.

WHY SMALL BUSINESSES ARE TARGETED

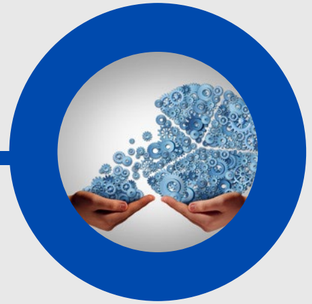
Access to sensitive government information

Intellectual property

Interconnection with larger defense contractors



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



Limited cybersecurity resources due to funding and are ill-prepared to handle cyber attacks

MANDATES AND REQUIREMENTS

- Stricter cybersecurity required by Defense Federal Acquisition Regulatory Supplement (DFARS) 252.204-7012, 252.204-7019 and 252.204-7020
- Updated National Institute Standards and Technology (NIST) Special Publication (SP) 800-171
  - NIST SP 800-31, 800-53, and 800-172 also may apply
- New cybersecurity regulations from U.S. Department of Homeland Security (DHS)
  - Reduction of Foreign Ownership, Control, or Influence (FOCI)
- Cybersecurity Maturity Model Certification (CMMC)
  - Version 2.0 – Increased focus on protecting sensitive data

A DEEPER DIVE ON CMMC 2.0

DoD created CMMC to protect the DIB's sensitive unclassified information from frequent and increasingly complex cyberattacks. CMMC 2.0 streamlined cybersecurity requirements:

- Simplifies compliance by allowing self-assessment for some requirements
- Applies priorities for protecting DoD information
- Reinforces cooperation between the DoD and industry in addressing evolving cyber threats

A DEEPER DIVE ON CMMC 2.0

- The Supplier Performance Risk System (SPRS) is the authoritative source to retrieve supplier and product performance information assessments for those in the DoD acquisition community to use in identifying, assessing, and monitoring unclassified performance.
- To achieve CMMC compliance, a company must upload a NIST SP 800-171 assessment score into the SPRS platform. This mandatory step verifies an organization's eligibility for federal contracts and ensures compliance with cybersecurity requirements.

CYBER ADVISORY SERVICES

- Our diverse Cyber Advisory Team is the engine that makes Project Spectrum tick – providing expertise in the following areas:
  - Compliance Services: Security Gap Analyses, Security System Plan (SSP) Assessment & Development, Plan of Action and Milestones (POAM) Assessment & Development, Security Enclave Design & Architecture Assessment
  - Cyber Advisory & Research Services: Technical Inquiries, MPP Cyber Pilot, Tool Research & Development
  - Education & Training: Content Creation, Compliance Training
  - Communications & Outreach: Blogs, Webinars, Videos

CYBERSECURITY TRAINING AND RESOURCES

Project Spectrum has developed a robust cybersecurity training program built upon our 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
- ‘Micro-courses’ that provide training on core CMMC controls
- DIY tools enabling companies to conduct self-assessments against NIST and CMMC standards to measure their current level of readiness prior to investing in CMMC certification pursuits.

NEXT-GEN CYBERSECURITY TOOL DEVELOPMENT

Project Spectrum's suite of next-generation tools will be used to prevent cyber threats and protect data

DECEPTION TECHNOLOGY

Generates realistic threat data, trains intrusion detection capabilities, and mitigates risk to systems/networks

SECURE CLOUD ENVIRONMENT

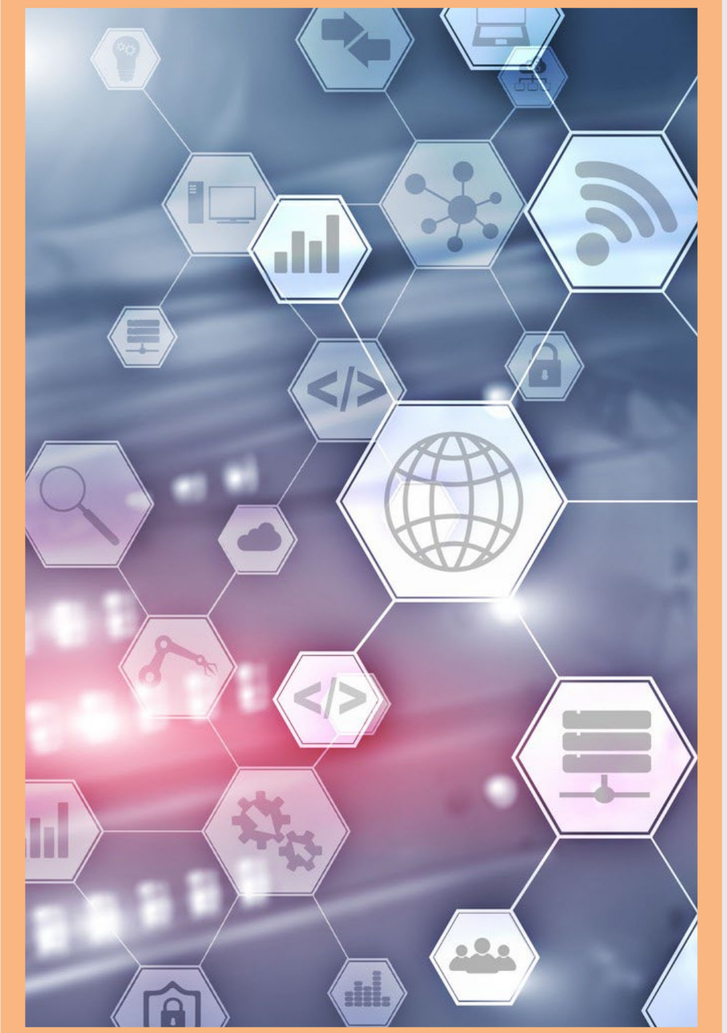
Provides secure storage, processing, and transmission of CUI through a virtual desktop

VISUAL NETWORK MAPPING

Vulnerability assessment tool that maps and replicates manufacturing networks and processes

POLYMORPHIC ENCRYPTION

Protects both data at rest and in motion based on user-specified conditions



CASE STUDY: SUCCESSFUL COMPLIANCE JOURNEY

- A small manufacturing company wanted to bid on a contract but lacked CMMC and DFARS compliance credentials
- The company reached out to Project Spectrum for guidance and registered for the MPP Pilot Program
  - Received access to technical/policy information and self-assessments
  - Tracked compliance journey progress on a customized dashboard
- PS Cyber Advisor (CA) worked with the company to develop a success plan to reach CMMC Level 1 and Level 2 compliance in 24 months:
  - Develop SSPs for CMMC Levels 1/2 and NIST 800-171;
  - generate POAMs; conduct initial SPRS assessment;
  - develop additional artifacts; identify and implement controls

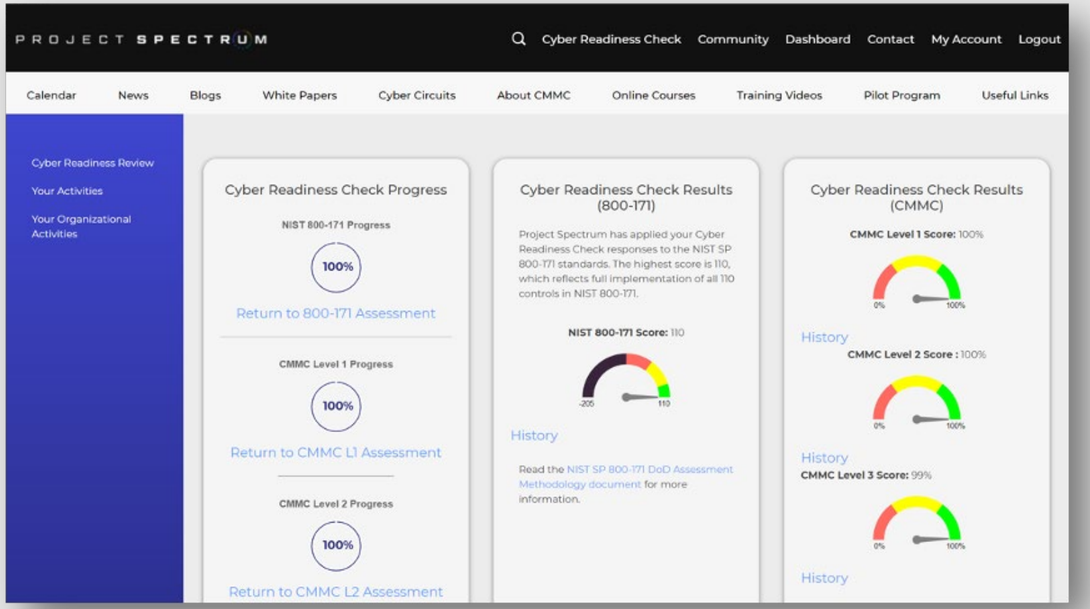
CASE STUDY: SUCCESSFUL COMPLIANCE JOURNEY

PS team took a very hands-on approach to help the company implement the plan

- Evaluated all documented claims against CMMC Level 1 controls
- Provided information on continuous monitoring devices and strategies to maintain compliance
- Reviewed Security Control Dashboard, Security Policy, Network Diagrams, CMMC Enclave Infrastructure Specifications
- Assisted with SSP and POAM development

CASE STUDY: SUCCESSFUL COMPLIANCE JOURNEY

- The company completed all steps to achieve CMMC and NIST SP 800-171 compliance
  - Developed enclave for all FCI and CUI data interaction
  - Created secure shared data repository
  - Developed an SSP and POAM for CMMC Level 2 and NIST SP 800-171



Result: a 30-point increase **in overall SPRS score**

CASE STUDY: SUCCESSFUL COMPLIANCE JOURNEY

Security Administrator Testimonial Highlights:

- The MPP Program cost the company nothing, but the CA team worked tirelessly on the company's behalf
- The takeaways were tremendous—reached CMMC Level 2 and increased SPRS score by more than 30 points
- CA team provided solid knowledge of the controls and helped the company build a stable Enclave infrastructure in a few months
- Bolstered SA's CMMC Compliance knowledge—assisted greatly with the company's ISO 27001 audit

INNOVATION, CYBERSECURITY, AND COMPLIANCE

- Project Spectrum can help small businesses increase compliance with cybersecurity standards and meet federal contracting guidelines and requirements
- Project Spectrum's tools, training, and resources are available at no cost to the user
- Improving cybersecurity can protect a small business' data, revenue, reputation, and intellectual property
- Increased cybersecurity throughout the small business community can protect the supply chain and our national security

CONNECT WITH US

OUTREACH@PROJECTSPECTRUM.IO

PROJECTSPECTRUM.IO

PROJECT SPECTRUM

PROJECT SPECTRUM

THANK YOU