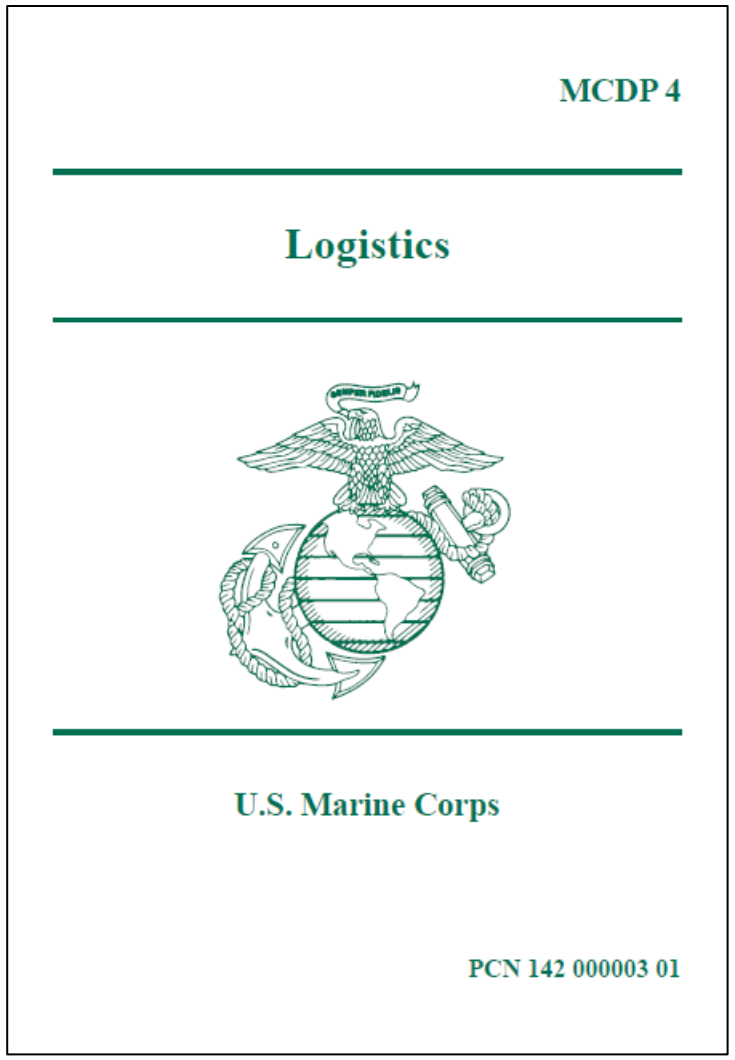
Contracting for Cybersecurity

Small DIB Contractors & Advanced Cyber Threats

Paul Shaw, DSc

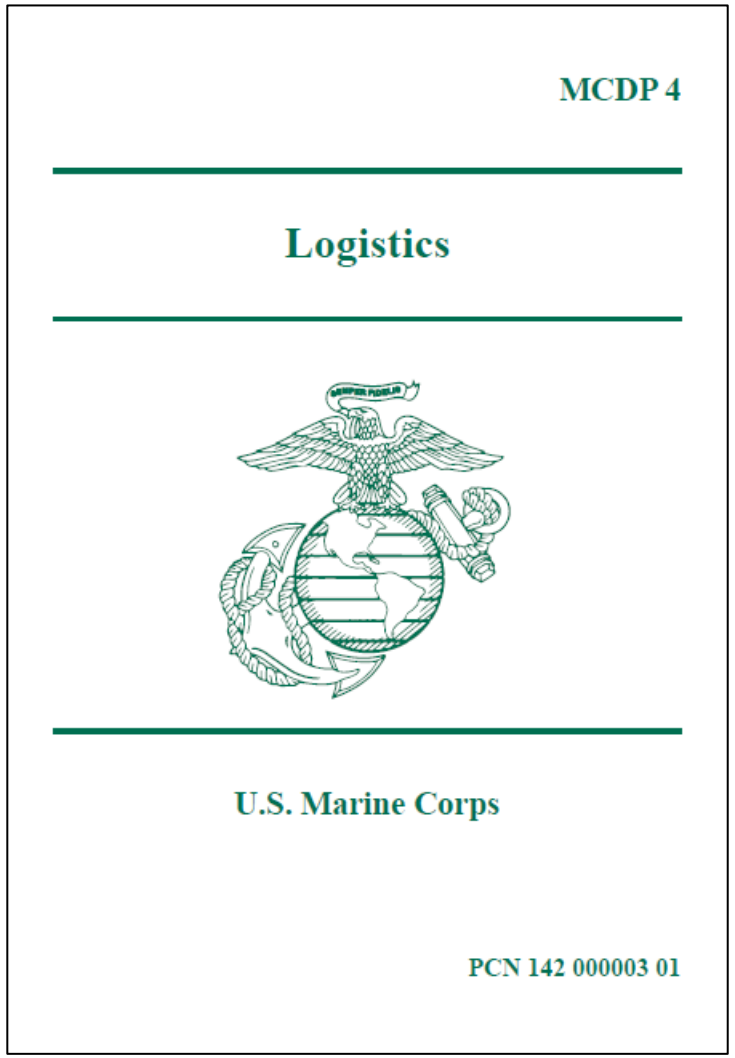
DAU

Cyber Threats



"Threats exist in all domains and the enemy will attack using every available weapon system and means to disrupt US operations. The enemy will use espionage, information functions, and space and cyberspace capabilities to rupture our cohesion and degrade our decision-making ability. These capabilities are so prevalent and important that space and cyberspace have been elevated to domains equal to land, maritime, and air. The space and cyberspace domains are particularly integral to global and regional logistics. Multi-domain operations provide opportunities for us to conduct logistics; however, they also provide the enemy opportunities to find, understand, and target logistics activities." (p.1-8)

Cyber Threats



"Threats to logistics capabilities may come in many forms across all domains. In physical form, a mobile or stationary logistics node can be targeted by conventional or special forces, insider threats, and non-state actors. Conventional forces using aviation assets, long-range fires, or space-based capabilities can target mobile or stationary logistics nodes over vast distances. Additionally, cyberspace attacks can deny or degrade communications among military forces and with supporting commercial partners. In great power competition, non-military tools such as economic or diplomatic coercion, can deny access to critical infrastructure such as ports, airfields, or host-nation supplies. Marines must have a comprehensive understanding of these threats to mitigate them through complementary, layered defensive measures and reconfigurable plans." (p.5-8)

Cyber Threats

MCDP 4

Logistics

U.S. Marine Corps

PCN 142 000003 01

Global Threats: Bill's Garage

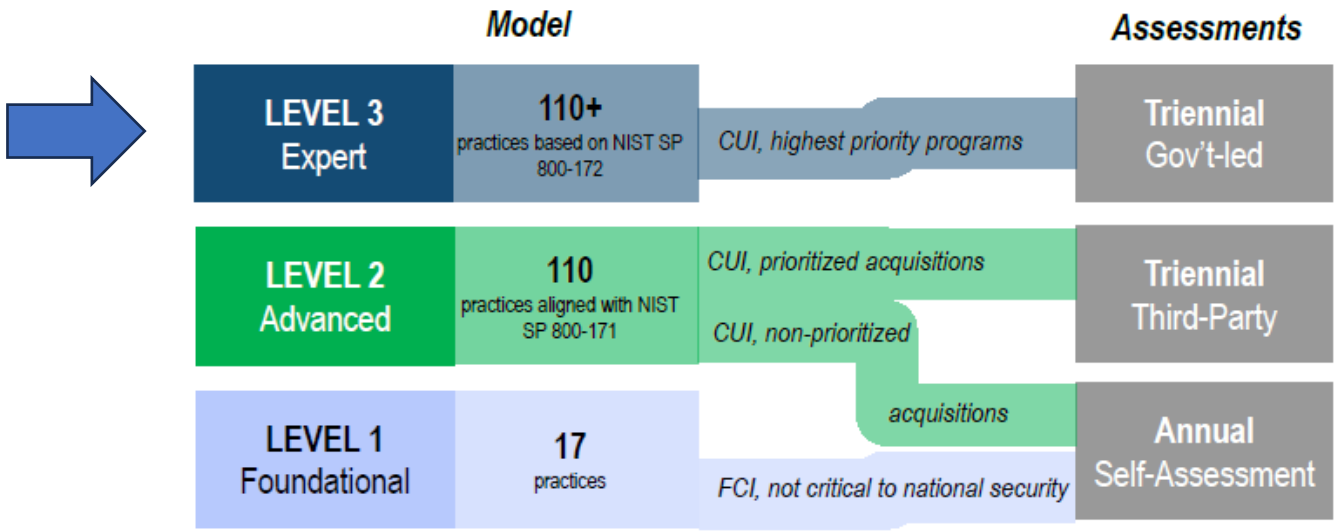
Bill lives in Grangeville, Idaho and runs a small manufacturing business. He is considered an expert in certain materiel solutions. In fact, Bill's ball bearings are so good, he received an exclusive contract to provide parts for an advanced weapons platform. Bill knows his bearings.

What Bill doesn't know is that a foreign country has a team of twelve people who monitor Bill's garage 24 hours a day. They can use the number of bearings that Bill provides the weapons manufacturers as indications and warnings as to whether the United States might attack them. This data is collected using a combination of satellite imagery, cyber monitoring, and human intelligence. Bill's garage is a priority target if tensions escalate because aircraft landing gear will not work without his bearings. A precision cyber strike is already in place to disrupt Bill's manufacturing business.

(p. 1-9)

Contracting Options

CMMC 2.0 tailors model and assessment requirements to the type of information being handled



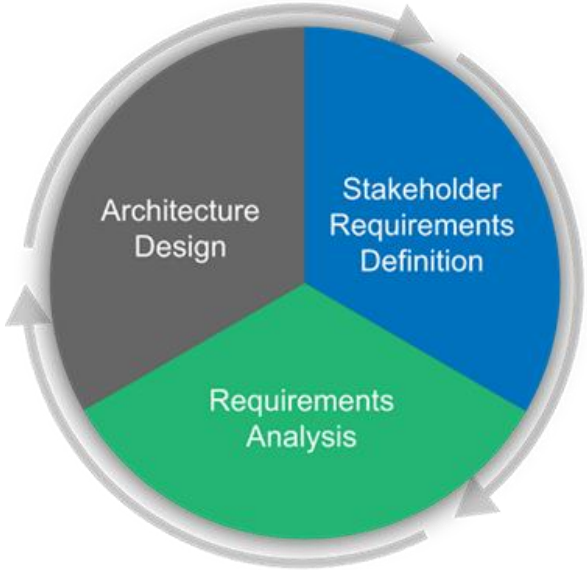
Note: The information in this presentation reflects the Department's strategic intent with respect to the CMMC program. The Department will be engaging in rulemaking and internal resourcing as part of implementation, and program details are subject to change during these processes.

As a Contracting Officer – would you assign a critical DIB Supplier who has extremely sensitive information to the "Expert" level?

Note: such an assignment requires NIST 800-171 security requirements and possibly some security requirements from NIST 800-172

OSD Slide from https://dodcio.defense.gov/Portals/0/Documents/CMMC/CMMC-2.0-Overview-2021-12-03.pdf

DIB Contractor



Purpose Statement

The purpose of this case study is to study implementation of advanced security controls for the Defense Industrial Base (DIB). The case study will use a small DoD contractor (approximately 500 employees or less) networked environment. This small DoD contractor has a hybrid network of on-premise cyber assets, commercial cloud, an isolated network, and a portion of their facility cleared for classified with connection to other networks (SIPRNet). They are a DoD “cleared for classified” in part of their facility. They have an air gapped network.

Contractor Profile

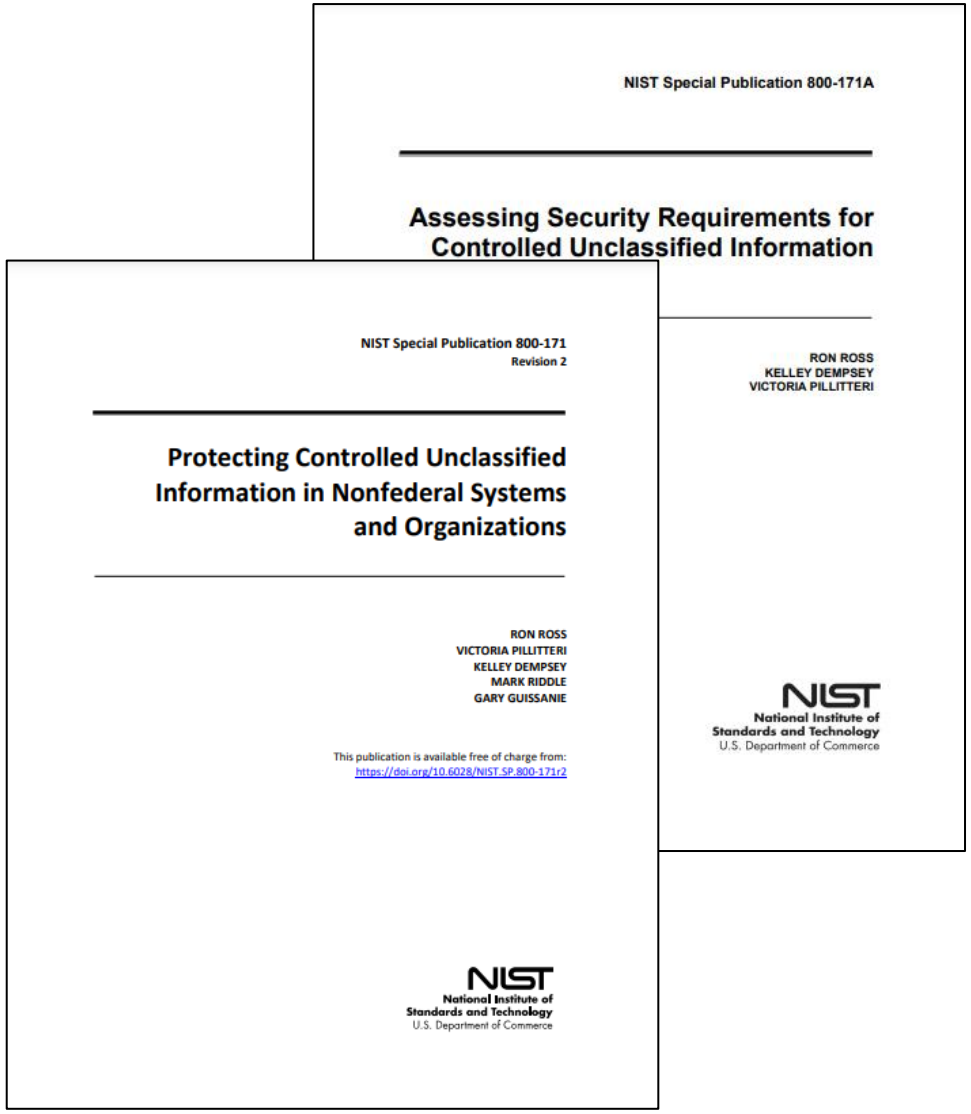
- Integrator of small space customized Nanosats. They need to maintain manufacturing control authority to counter potential advanced nation state actors who might want to steal their information & disrupt their manufacturing process.
- This company received recent threat warnings of a nation state actor possibly targeting them.
- Due to having “Highly Sensitive CUI” - this company implemented the NIST 800-171 and NIST SP 800-172 security requirements. To assess implementation of their security requirements, they used the NIST 800-171A and NIST SP 800-172A for assessment.
- Note: their highly sensitive unclassified information has one or more of the following markings: Controlled Unclassified Information (CUI); Controlled Technical Information (CTI); National Security System (NSS); and International Traffic in Arms Regulations (ITAR).

Profile

Corporate profile:

- A company under 500 employees that manufactures custom Nanosats for the DoD, NASA, US allies, & commercial companies (such as Starlink). One of a few manufacturers who can make such custom components.
- Microsoft Windows on internal corporate servers & most endpoint devices. Use Microsoft's automated patching service.
- Allows user endpoint devices to communicate with the company network, to include IPhones, Tablets, & personal computers. Some employees telework from personal computers.
- They have team of trained cybersecurity personnel who form a Security Operations Center (SOC) with SIEM capabilities of analyzing existing log files. They would like to comply with the DoD's Zero Trust Capability of "Threat Intelligence Integration." Their objective is to automate and improve their capabilities to counter advanced threats.

Guiding Documentation



NIST Special Publication 800-171A

Assessing Security Requirements for Controlled Unclassified Information

RON ROSS
KELLEY DEMPSEY
VICTORIA PILLITTERI

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NIST Special Publication 800-171
Revision 2

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

RON ROSS
VICTORIA PILLITTERI
KELLEY DEMPSEY
MARK RIDDLE
GARY GUISSANIE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-171r2

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NIST Special Publication 800-172A

Assessing Enhanced Security Requirements for Controlled Unclassified Information

RON ROSS
VICTORIA PILLITTERI
KELLEY DEMPSEY

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-172A

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NIST Special Publication 800-172

Enhanced Security Requirements for Protecting Controlled Unclassified Information

A Supplement to NIST Special Publication 800-171

RON ROSS
VICTORIA PILLITTERI
GARY GUISSANIE
RYAN WAGNER
RICHARD GRAUBART
DEB BODEAU

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-172

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

DAU

NIST 800-172 Requirement – Security Operation Center

NIST 800-172 Enhanced Security Requirement – Incident Response 3.6.1e

Establish and maintain a security operations center capability that operates [Assignment: organization-defined time period].

A security operations center (SOC) is the focal point for security operations and computer network defense for an organization. The purpose of the SOC is to defend and monitor an organization's systems and networks (i.e., cyber infrastructure) on an ongoing basis. The SOC is also responsible for detecting, analyzing, and responding to cybersecurity incidents in a timely manner. The SOC is staffed with skilled technical and operational personnel (e.g., security analysts, incident response personnel, systems security engineers); in some instances operates 24 hours per day, seven days per week; and implements technical, management, and operational controls (e.g., monitoring, scanning, and forensics tools) to monitor, fuse, correlate, analyze, and respond to security-relevant event data from multiple sources. Sources of event data include perimeter defenses, network devices (e.g., gateways, routers, and switches), and endpoint agent data feeds. The SOC provides a holistic situational awareness capability to help organizations determine the security posture of the system and organization. An SOC capability can be obtained in many ways. Larger organizations may implement a dedicated SOC while smaller organizations may employ third-party organizations to provide such a capability.

NIST 800-172 Requirement – Threat Indicators

NIST 800-172 Enhanced Security Requirement - System and Information Integrity 3.14.6e

Use threat indicator information and effective mitigations obtained from [Assignment: organization-defined external organizations] to guide and inform intrusion detection and threat hunting.

Threat information related to specific threat events (e.g., TTPs, targets) that organizations have experienced, threat mitigations that organizations have found to be effective against certain types of threats, and threat intelligence (i.e., indications and warnings about threats that can occur) are sourced from and shared with trusted organizations. This threat information can be used by organizational Security Operations Centers (SOC) and incorporated into monitoring capabilities. Threat information sharing includes threat indicators, signatures, and adversary TTPs from organizations participating in threat-sharing consortia, government-commercial cooperatives, and government-government cooperatives (e.g., CERTCC, CISA/US-CERT, FIRST, ISAO, DIB CS Program). Unclassified indicators, based on classified information but which can be readily incorporated into organizational intrusion detection systems, are available to qualified nonfederal organizations from government sources.

DoD ZT Capabilities

6.7	Security Operations Center (SOC) & Incident Response (IR)	7 - Visibility and Analytics 6 - Automation and Orchestration	In the event a computer network defense service provider (CNDSP) does not exist, DoD organizations define and stand up security operations centers (SOC) to deploy, operate, and maintain security monitoring, protections and response for DAAS; SOCs provide security management visibility for status (upward visibility) and tactical implementation (downward visibility). Workflows within the SOC are automated using automation tooling and enrichment occurs between service providers and technologies.	In the event a CNDSP does not exist, DoD organizations define and stand up SOCs to deploy, operate, and maintain security monitoring, protections and response for DAAS; SOCs provide security management visibility for status (upward visibility) and tactical implementation (downward visibility)	Standardized, coordinated, and accelerated incident response and investigative efforts	* Workflow Enrichment Pt1 * Workflow Enrichment Pt2 * Workflow Enrichment Pt3 * Automated Workflow

ID #	Capability	Pillar	Capability Description	Capability Outcome	Impact to ZT	Activities
7.2	Security Information and Event Management (SIEM)	7 - Visibility and Analytics	Computer Network Defense Service Provider (CNDSP) or security operations centers (SOC) monitor, detect, and analyze data logged into a security information and event management (SIEM) tool. User and device baselines are created using security controls and integrated with the SIEM. Alerting within the SIEM is matured over the phases to support more advanced data points (e.g., Cyber Threat Intel, Baselines, etc.)	CNDSPs/SOCs monitor, detect, and analyze data logged into a security information and event management (SIEM) tool	Processing and exploiting data in the SIEM enables effective security analysis of anomalous user behavior, alerting, and automation of relevant incident response to common threat events	* Threat Alerting Pt1 * Threat Alerting Pt2 * Threat Alerting Pt3 * Asset ID & Alert Correlation * User/Device Baselines
			anomalies.			
7.5	Threat Intelligence Integration	7 - Visibility and Analytics	Computer Network Defense Service Provider (CNDSP) or security operations centers (SOC) integrate threat intelligence information and streams about identities, motivations, characteristics, and tactics, techniques and procedures (TTPs) with data collected in the SIEM.	CNDSPs/SOCs integrate threat intelligence information and streams about identities, motivations, characteristics, and tactics, techniques and procedures (TTPs) with data collected in the SIEM	Integrating threat intelligence into other SIEM data enhances monitoring efforts and incident response	* Cyber Threat Intelligence Program Pt1 * Cyber Threat Intelligence Program Pt2

DoD Zero Trust Execution Roadmap, p. 56 & 57

Application Threat Protections

The CISA Zero Trust Maturity Model for “Application Threat Protections” is shown below. Your goal is to achieve “Advanced” Application Threat Protection for the Zero Trust Capability of “Threat Intelligence Integration.”

Function	Traditional	Initial	Advanced	Optimal
Application Threat Protections	Agency threat protections have minimal integration with application workflows, applying general purpose protections for known threats.	Agency integrates threat protections into mission critical application workflows, applying protections against known threats and some application-specific threats.	Agency integrates threat protections into all application workflows, protecting against some application-specific and targeted threats.	Agency integrates advanced threat protections into all application workflows, offering real-time visibility and content-aware protections against sophisticated attacks tailored to applications.

Meeting with the Company

The company wants to use the DoD Zero Trust capability of “Threat Intelligence Integration” with their SOC and their current concept of “threat indicators” from the NIST 800-172 security requirement (Requirement 3.14.6e).

They would like to establish better Security Operation Center (SOC) analysis. They are hoping to automate analysis to the maximum extent possible. They currently use threat intelligence feeds from CISA/US-CERT and the DIB CS Program. Their SOC has a commercial SIEM license with Splunk. They consider that sufficient to meet the intent of the DoD’s Zero Trust “Threat Intelligence Integration” capability. The contractor rates their maturity using the CISA Maturity Model (on the next slide) as “Initial.” They claim to want to progress to an “Advanced” CISA Maturity Rating for “Application Threat Protection.”

Discussion

As a Contracting Officer, do you agree with their approach? Since they followed DoD policy and guidance, do you have any concerns? Was there any concerns with the contractor talking to other DoD representatives?

Contractor's first question – what is reimbursable of their implementation?

- Current facts – your original work with the Contractor was part of an OTA managed by the "Space Consortium"
- Follow-on contract for a particular project was a firm fixed price