

Supply Chain Cybersecurity Risk Management for Construction and Maintenance Projects



USG shutdown precluded this earlier-submitted presentation from occurring

Learning Objectives

- Definition of SCRM in cybersecurity
- Importance of protecting vendor-to-end-user pathways
- Growing attack surface in global supply chains

Agenda

- Risk Management and Strategies for Supply Chain Risk Management (SCRM)
- Challenge 1 - Understanding the Supply Chain Risk
- Challenge 2 – The Importance of Standardized Requirements
- Real-World Examples
- What is the End State / Q&A / Discussion

What is Supply Chain Risk Management ?



Supply Chain Risk Management (SCRM)

- Cybersecurity for SCRM focuses on identifying, assessing, and mitigating risks associated with suppliers, contractors, and service providers.
- As supply chains become more interconnected and reliant on digital systems, attackers find more entry points. A single weak vendor can compromise the entire chain.



SCRM SUPPLY CHAIN RISK MANAGEMENT

Common Cyber Risks in Supply Chains

- Compromised hardware or software components
- Insider threats within suppliers
- Data breaches from third-party networks
- Malware-infected updates or patches



Key SCRM Cybersecurity Strategies

- Vet and monitor suppliers continuously
- Require adherence to cybersecurity standards (e.g., NIST, ISO 27001)
- Implement multi-factor authentication and least-privilege access
- Conduct regular security audits and penetration tests

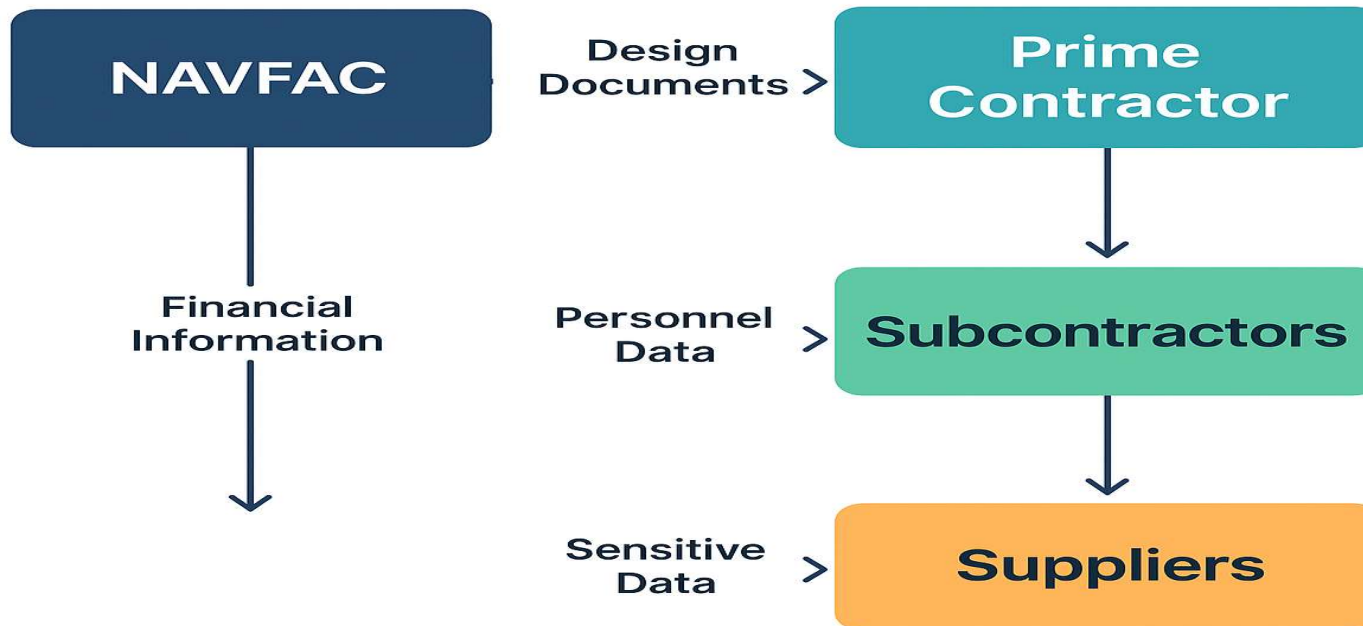


Threats can be intentional or accidental. For example, malicious code injected during manufacturing, or a supplier's poor security allowing hackers access to sensitive data. Even routine updates, if not verified, can deliver malware to multiple customers at once.

Challenge 1: Understanding the Supply Chain Risk



Example of SCRM Ecosystem





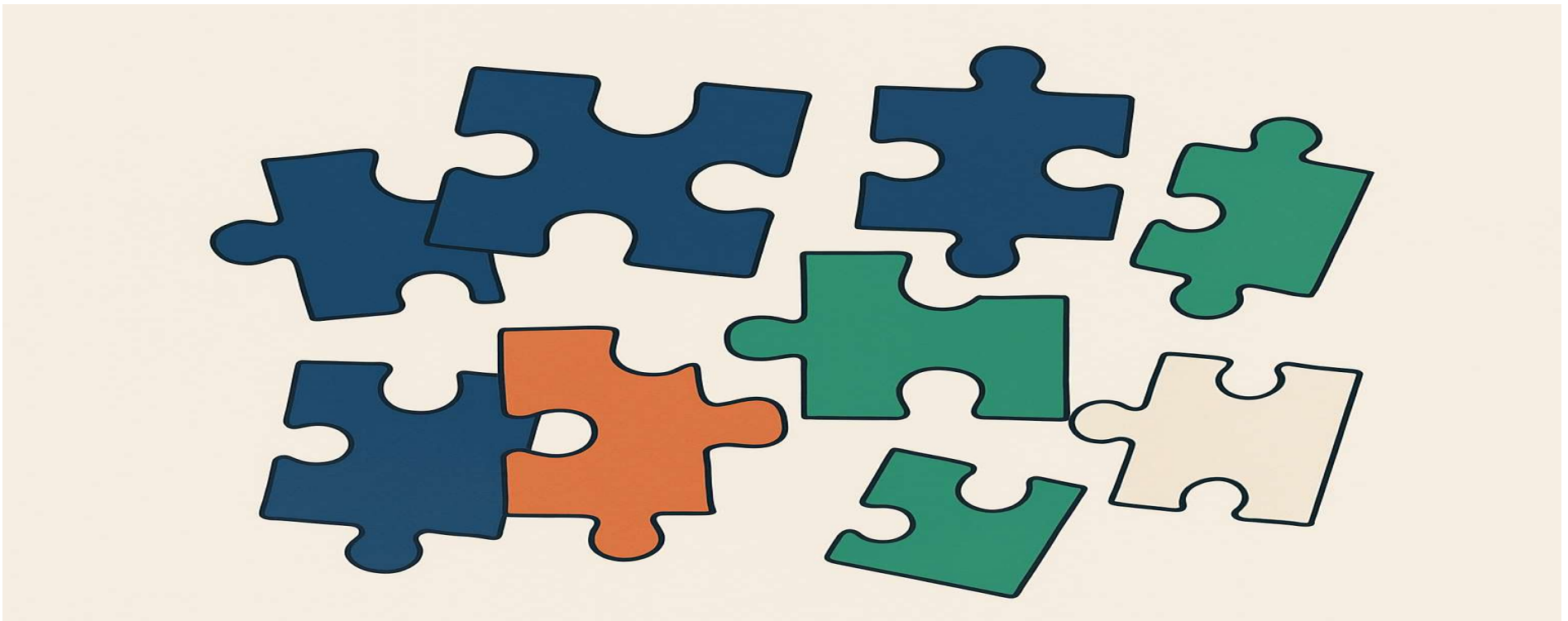
Challenge 1: Understanding the Supply Chain Risk

- **The Expanding Attack Surface:** NAVFAC relies on a vast network of contractors and subcontractors to design, build, and maintain critical naval facilities. Think of it like a chain – the entire chain is only as strong as its weakest link.
- **Complexity = Vulnerability:** The more participants involved in a project, the greater the chance that one or more entities will have weak cybersecurity practices.
- **Potential Impact of a Successful Cyberattack:**
 - **Data Breach:** Loss of sensitive project data, including design plans, financial records, and personnel information. This could compromise national security, violate privacy regulations, and damage NAVFAC's reputation.
 - **Project Delays:** Disruption of construction or maintenance activities due to ransomware attacks, data corruption, or system outages.
 - **Financial Loss:** Direct costs associated with incident response, data recovery, and legal liabilities. Indirect costs can include loss of productivity and damage to NAVFAC's brand.
 - **Reputational Damage:** Loss of trust from stakeholders, including government agencies, contractors, and the public.

Challenge 2: The Importance of Standardized Requirements



Standardized Cybersecurity Requirements



Challenge 2: The Importance of Standardized Requirements

- **The Problem with Inconsistency:** Without standardized cybersecurity requirements, contractors operate with varying levels of security, creating significant vulnerabilities across the NAVFAC supply chain. This increases the risk for everyone.
- **Why Standardized Requirements are Crucial:**
 - **Reduced Risk:** Consistent security standards across the supply chain reduce the overall risk of cyberattacks.
 - **Improved Compliance:** Clear and enforceable requirements make it easier for contractors to comply with NAVFAC's security expectations.
 - **Easier Monitoring:** Standardized requirements allows the ability to effectively monitor contractor security posture and identify potential weaknesses.
 - **Enhanced Accountability:** Clear requirements make contractors accountable for maintaining a specific level of security.
- **Analogy:** Think of it like building codes. Standardized building codes ensure that all buildings meet a minimum level of safety and quality. Standardized cybersecurity requirements do the same for information security.

"Imagine a construction site where some workers follow safety rules and others don't. That's the situation we face with cybersecurity if we don't have standardized requirements."

"Standardized requirements are not just about compliance; they're about protecting critical assets and ensuring the success of our projects."

"By leveling the playing field, we create a more secure and resilient supply chain. ."

Real-World Examples



SolarWinds Orion attack (2020)



Major cyberespionage incident attributed to the Russian Federation. Hackers used a supply chain attack, inserting malicious code into updates for SolarWinds' Orion software, which was then downloaded by thousands of organizations, including U.S. government agencies like the Department of Defense and Treasury.

Target Data Breach (2013) via HVAC Contractor



In Target's breach, the attackers entered via a third-party HVAC contractor. Breach involved hackers accessing Target's systems through a third-party vendor, leading to the compromise of personal and credit card information for approximately 110 million customers during the busy holiday shopping season

NotPetya Ransomware 2017 Spreading through Software Update



Estimated to be more than \$10 billion by the U.S. government, though company-reported losses initially focused on a smaller figure in the hundreds of millions. The attack inflicted massive financial and operational damage by disrupting critical infrastructure and businesses worldwide

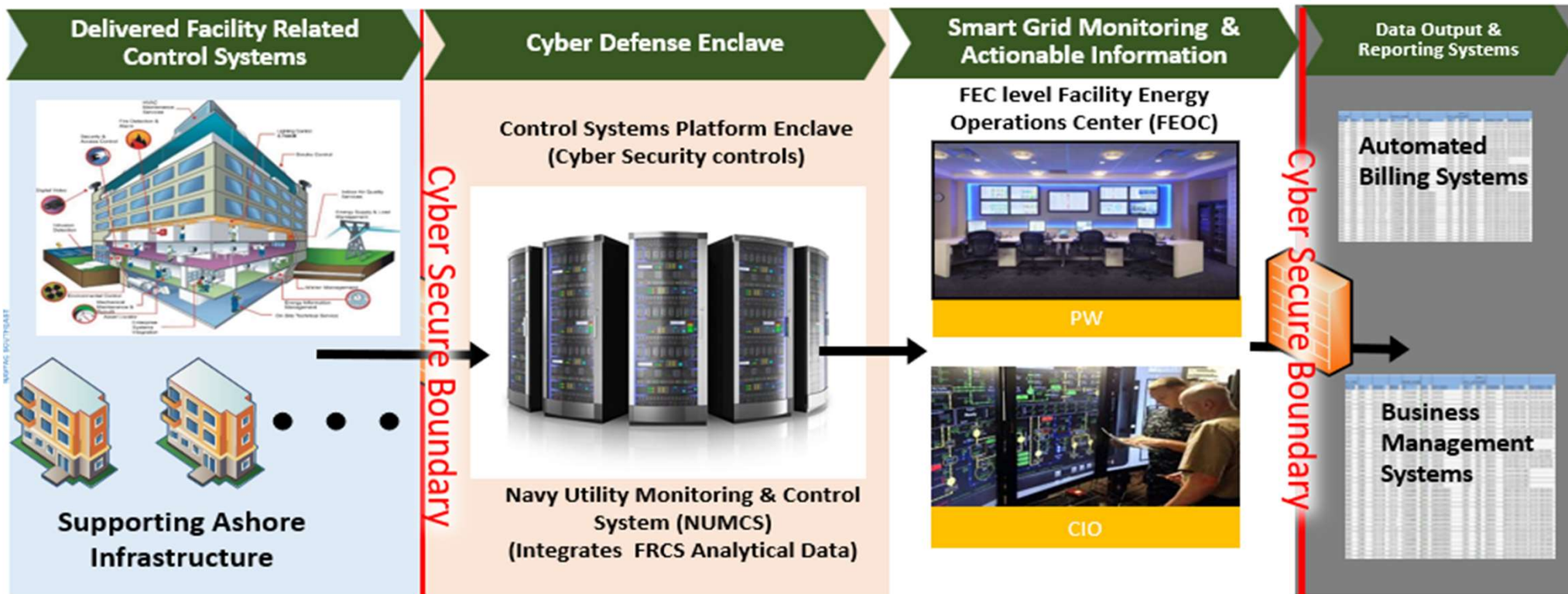


What's NAVFACs End-State.

Resilient and Reliable FRCs

1. **Delivered FRCs:** (Facility turned over to PW) NAVFAC SE (PW8, PWD Operators, CIO4 and CIO2) is responsible for the Reliability and Resiliency of FRCs inventory and sustainment in which NAVFAC is the Utility or Maintenance owner. *Note: FRCs in which NAVFAC are the "Maintenance Owner Only" the Cyber support (RMF, continuous monitoring and patching, etc.) should be paid by the Facility Owner (i.e. CNIC, BUMED, etc).*
2. **Cyber Secure Boundary:** represents the "CSPE 2" defense infrastructure environment
3. **Cyber Defense Enclave:** CIO Centralized Cyber Security services (patching, updating, and monitoring) for OT components (Resiliency) – minimize cyber attacks and impact to mission (FRCs Connected to CSPE2)
4. **Smart Grid Monitoring & Actionable Information:** PW/CIO FRCs Monitoring and Energy Management (Reliability) - minimal operation impacts
5. Smart Grid is NAVY'S Solution for Building Control Systems/Utility Control Systems to:
 1. Cybersecuring at lowest Total Operating Costs
 2. Energy Reduction through data analysis
 3. Predictive Maintenance
6. **Data Output & Reporting Systems**– Secure transport of data to business systems

The End State



CIO Cybersecurity POCs



CYBERSECURITY PROGRAM OVERSIGHT

CIO2 CYBERSECURITY MANAGEMENT



CIO2: William Smiley
Cybersecurity Division Director
904-542-9056 | william.l.smiley4.civ@us.navy.mil



CIO: Andrea Freeman
Command Information Officer
904-542-4191 | andrea.l.freeman.civ@us.navy.mil

CIO4 CYBERSECURITY INFRASTRUCTURE AND ENGINEERING



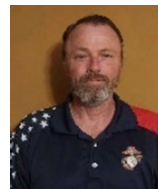
CIO4: Antonio Jefferson
Operation Technology Division Director
904-542-5839 | antonio.s.jefferson2.civ@us.navy.mil



CIO2.1: Lydell Sapp
Construction and Design Contracts Review /
Cybersecurity Commissioning (CyCx)
904-542-8484 | Lydell.d.sapp.civ@us.navy.mil



CIOD: Joseph Ellis
Defensive Cybersecurity Operations
Analyze Cyber Threats and Vulnerabilities
(904) 403-8323 | joseph.p.ellis.civ@us.navy.mil



CIO41: Bobby Kelley
Control Systems Platform Enclave Brch Manager
ACAS, HBSS and VMWARE Support
904-542-2490 | bobby.j.kelley.civ@us.navy.mil



CIO42: Kevin Gaddist
Facilities Related Control Systems Brch Manager
AMI, SCADA, DDC, and HVAC Support
904-542-8495 | kevin.k.gaddist.civ@us.navy.mil



CIO43: Paddy Jackson
Information Systems Security Engineer Lead
DRAGOS / Cybersecurity Threat Analysis
904-542-5488 | paddy.o.jackson.civ@us.navy.mil

Q&A / Discussion

