International Council on Systems Engineering
A better world through a systems approach

A Proposed Capability Package for Preventing Hardware-Specific Cyber Attacks in Critical Infrastructure

Irem Gultekin Chiappone, Ph.D. Candidate

Reginald U. Bailey, Ph.D.

This material is abstracted from a dissertation currently in work for The George Washington University in partial fulfillment of the requirements for the Doctor of Philosophy degree.

INCOSE International Symposium 2025 | Ottawa, Canada

About the Speaker

RIT

Rochester Institute of Technology

THE GEORGE WASHINGTON UNIVERSITY

WASHINGTON, DC

amazon

Today's Agenda

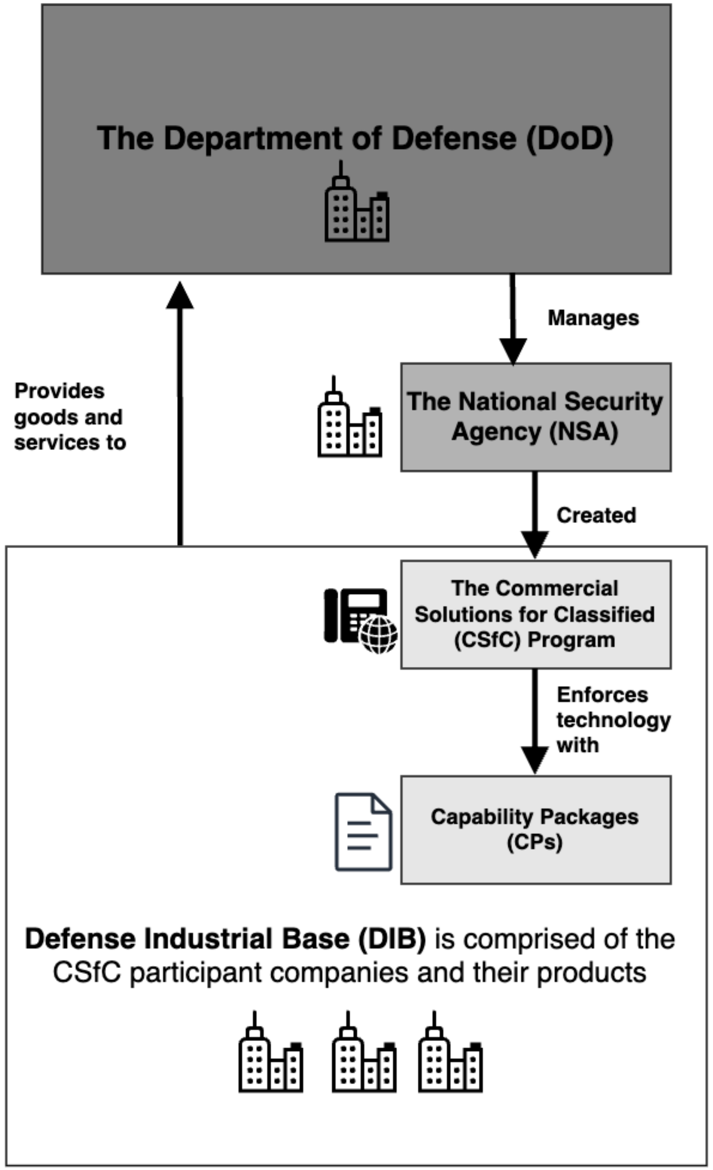
1. **Introduction**
2. Research Motivation, Challenges
3. Problem Statement, Proposed Solution
4. What Success Looks Like, Intended Benefits
5. Research Methods
6. Preliminary Findings and Capability Package Framework
7. Conclusion & Next Steps
8. **Q&A**

Introduction

The Defense Industrial Base: Over 300,000 professionals, critical in protecting national security.

Capability Packages:

- Developed by NSA/DoD to help implement secure solutions in classified environments
- Includes: threat scenarios, configuration guidance, implementation options
- They are both prescriptive and adaptable, helping reduce ambiguity in complex systems.
- We propose adapting this concept to hardware cybersecurity for the Defense Industrial Base (DIB), which in turn provides technology, products, and services to the DoD.


The Department of Defense (DoD)
Manages
The National Security Agency (NSA)
Provides goods and services to
Created
The Commercial Solutions for Classified (CSfC) Program
Enforces technology with
Capability Packages (CPs)
Defense Industrial Base (DIB) is comprised of the CSfC participant companies and their products

Introduction

***Fig 1:** Satellite relay to space vehicles. Credit: SpaceLink (eosspacelink.com)*

Why Focus on the Defense Industrial Base (DIB)?

- Heavy Reliance on Classified Communication: DIB uses CSfC-approved components more than any other critical infrastructure sector.
- Complex Supply Chain & Integration Environment: Thousands of contractors and subcontractors each possessing different levels of security maturity.
- Lack of Unified, Prescriptive Hardware Security Guidance: Existing standards (NIST, CMMC) focus largely on software or policy; DIB needs specific guidance for hardware protection.

Research Motivation & Current Challenges

Where Existing Frameworks Fall Short

Framework	Focus	Hardware Coverage	Applicability to DIB
NIST 800-53	Broad cybersecurity controls	Minimal hardware-specific guidance	Partially useful
CMMC	Supply chain and maturity	Software-heavy, light on hardware	Some relevance
CSfC	Classified comms	Strong, but classified use only	Not open to industry
CISA Best Practices	General awareness	Reactive, non-prescriptive	Inconsistent uptake

Problem Statement & Proposed Solution

Current Problems

- Defense Industrial Base (DIB) comprises hardware and integrated systems for classified communication, including:
  - **Satellite relays**
  - **Missile defense systems**
  - **The military**
  - **Defense contractors**
- Despite growing threats, hardware-specific cybersecurity methodologies remain underdeveloped.

Proposed Solution

- Framework, based on CSfC's Capability Package (CP) for ease of use and guidance.
- Fill the gaps with critical hardware methodologies based on research on the latest vulnerabilities and attacks.
- Make it easier for DIB stakeholders to **respond** to attacks, **choose** and **implement** security methodologies.

What Success Looks Like

Give industry a powerful hardware security framework

A Successful Outcome

- **Borrow from DoD Capability Packages:** hardware developed for classified use already adhere to security-focused, prescriptive design goals managed by the DoD
- **DIB classified communications hardware needs the same**
- A validated, centralized framework for hardware cybersecurity methodologies
- Clear value in reducing the time to research and implement ambiguous cybersecurity methodologies
- Reference cases for proven success and long-term security and safety
- Tools that align cybersecurity methods with specific system architectures.

The Intended Benefits

- **Accelerates Adoption of Best Practices:** Simplifies navigation of fragmented hardware security guidance across the DIB.
- **Promotes Consistency and Alignment:** Establishes a shared framework for defense contractors and agencies..
- **Leverages Real-World Evidence:** Bases recommendations on validated, research-backed case studies.
- **Supports Clearer, Faster Decisions:** Links security measures to specific systems, risks, and use cases.
- **Strengthens National Cyber-Physical Resilience:** Closes critical gaps in the hardware layer of defense infrastructure.

Research Methodology

Provide value to DIB with a powerful security framework

Hypotheses

- CPs improve detection and mitigation of hardware threats.
- CPs reduce large-scale hardware-related disruptions.
- CPs enable proactive hardware security.
- CPs standardize incident reporting.
- CPs are adaptable from DoD/NIST to industry.

Research Methods

- Literature Review
- Framework Gap Analysis
- Case Study Analysis
- Expert Interviews

Fig 2: *Secure communications terminal operators. Credit: L3Harris (l3harris.com)*

Preliminary Findings

How the CP will work and how the DIB could benefit from its use

Results:

- Many DIB organizations have different approaches, especially when no framework exists.
- Companies make up their own solutions, may or may not be best for the scenario. **Example:** Maersk rebuilt their entire network, then implemented honeypot methods.
- Categorization of methodologies for best results:

  Preventative: Preventative design and hardening techniques.

  Reactive: Incident response and mitigation strategies.

  Honey Pot: Controlled environments for monitoring attackers during the attack.
- There may be strategic benefits in allowing an attack to run its course while monitoring it in real time.

How the CP Works:

- Validation of methodologies through case studies, expert reviews, and alignment with existing policy.
- Framework for selection based on criteria correlating it to effectiveness against attack, each firm.
- Updated with the latest research findings turned into prescriptive methodologies, refreshed periodically by a public or private owner.
- No ambiguity on ownership and updating.

Conclusions & Next Steps

Future work to build off what we've learned

Conclusions:

- **The effectiveness criteria** for choosing solutions needs to be improved for deeper correlation to desired outcomes, types of firms, business structures, risk profiles, etc.
- Additional defense categories, more applicable to certain types of attack, need to be considered in order to fit a wide array of attack types

What's Next:

- Refine the approach to validating methodologies (case studies, expert review, policy alignment)
- **Ownership, management, and upkeep discussions:** who is best suited for keeping the record up to date?
- Applications within other industries in DIB beyond classified communication hardware, other critical infrastructure
- Weaknesses in the CP solution and alternatives, fixes for those weaknesses

Thank you!
Q&A

Irem Gultekin Chiappone, Ph.D. Candidate

iremg@gwmail.gwu.edu