Engaging the DoD Enterprise to Protect U.S. Military Technical Advantage

Brian Hughes
Office of the Deputy Assistant Secretary of Defense for Systems Engineering

19th Annual NDIA Systems Engineering Conference
Springfield, VA | October 24, 2016

Bottom Line Up Front

- ✓ Adversary is targeting our Controlled Technical Information
- ✓ This audience is not only critical to protecting that information but helping DoD identify which information it should protect
- ✓ Significant amount of technical expertise resides in the DIB

Partnership between DoD and DIB is vital

Agenda

- **DoD efforts to safeguard Controlled Technical Information (CTI)**
- **Tailored engagements**
- **Tunable Response Options**
- **Defense Industrial Base (DIB)'s role in the process**

Addressing the Loss of CTI

Risk = f (threat, vulnerabilities, consequences)

Goals:

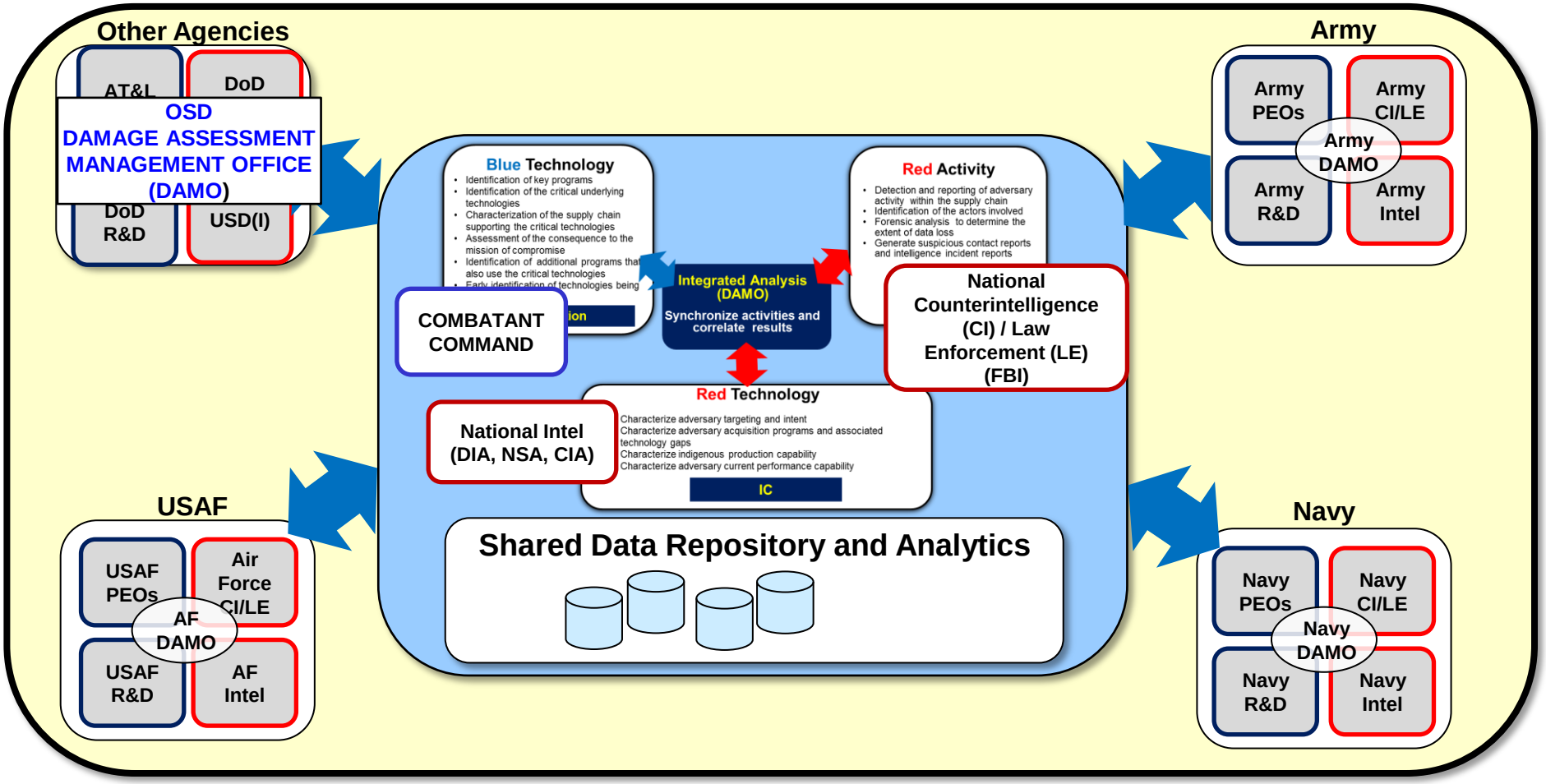
- **Enable information-sharing, collaboration, analysis, and risk management between acquisition, LE, CI, and IC**
  - Connect the dots in the risk function (map blue priorities, overlay red threat activities, warn of consequences)
- **Integrate existing acquisition, LE, CI, and IC information to connect the dots in the risk function - linking blue priorities with adversary targeting and activity**
  - Many sources and methods are relevant (e.g., HUMINT, joint ventures)
  - Cyber is only one data source
- **Focus precious resources**
- **Speed discovery and improve reaction time**
- **Ultimately, evolve to a more proactive posture**

JAPEC Mission: Integrated Analysis

The Joint Acquisition and Protection Cell (JAPEC) integrates and coordinates analysis to enable Controlled Technology Information (CTI) protection efforts across the DoD enterprise to proactively mitigate future losses, and exploit opportunities to deter, deny, and disrupt adversaries that may threaten US military advantage.

JAPEC: Integrating Analysis done at the Enterprise-Level

JAPEC



Agenda

- DoD efforts to safeguard Controlled Technical Information (CTI)
- **Tailored engagements**
- Tunable Response Options
- Defense Industrial Base (DIB)'s role in the process

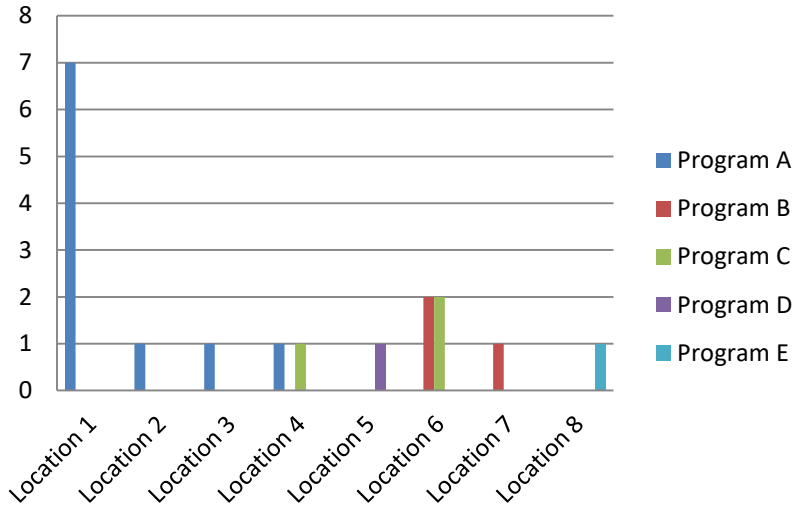
Tailored Engagements: Dialogue with Protection Stakeholders

- **Compliance with existing rules and regulations is necessary but not sufficient**
  - Protection is more than completing a checklist
- **What is crucial to your organization delivering the desired capability?**
  - Identify who, what and where at each facility
    - FSO may not be well positioned to speak to this
  - Are there links with other programs, especially if the programs are in a different Military Department?
    - Informing all involved parties helps focus IC, CI, and LE resources
  - Are there plans to market the same technology to other Military Departments or Government Agencies?
    - Government regulations and laws protect business proprietary

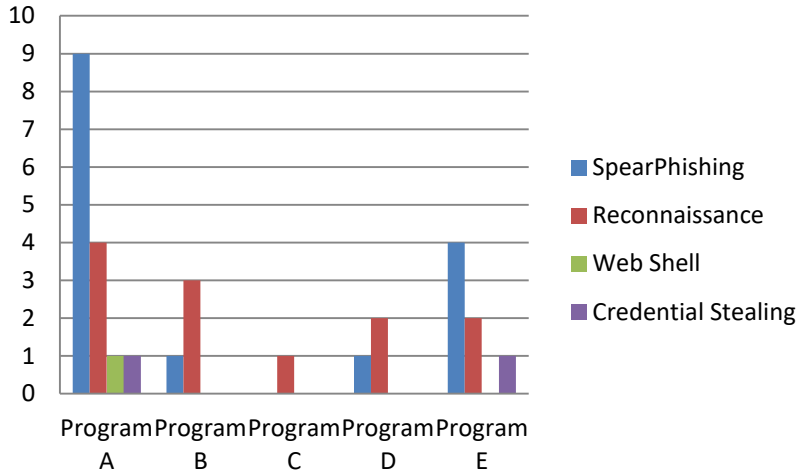
Adversary is Dynamic and Active

Working an All Source Problem

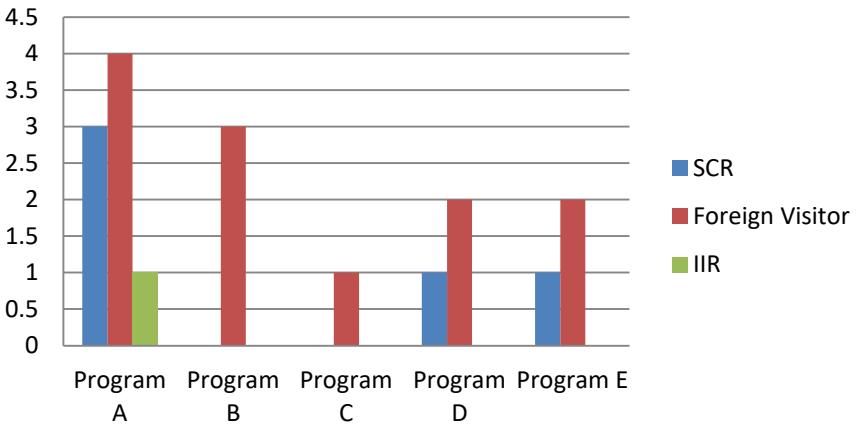
Stolen Media Incidents



Known Cyber Incidents



CI Activity



- Is a program targeted?
  - By whom? For what reason?
- Who is putting these pieces together to answer that question?
  - The data does not exist in this format – you have to make it usable
- What actions can be taken?

Agenda

- DoD efforts to safeguard Controlled Technical Information (CTI)
- Tailored engagements
- **Tunable Response Options**
- Defense Industrial Base (DIB)'s role in the process

Tunable Response Options

- **Acquisition**
  - Contract language
  - Threat education
  - Make program adjustments
    - e.g., accelerate alternative technologies
  - Develop in classified environment
- **Counterintelligence**
  - Awareness training for programs (DIB/Government Program Offices)
  - Incident investigations
  - Focused CI support to security programs
- **Intelligence Community**
  - Focused collection
- **Research and Development**
  - Contract language
  - Threat education
  - Rapid classification
- **CIO / Network Security**
  - Tiered IT security controls (e.g. isolated networks, commercial encryption)
- **Requirements Community**
  - Revise requirements based on change in threat
- **Warfighter**
  - Accept greater mission risk
  - Update Tactics/Techniques/Procedures (TTPs)

Threat Education

- **Engage LE/CI assets with sufficient context to link events**

STOLEN MEDIA INCIDENTS	ADDITIONAL DETAIL
1. Laptop stolen - Employee's vehicle was parked in the hardware supply parking lot 2. Laptop and laptop bag were discovered stolen from the trunk of the employees personal parked vehicle 3. Employee reported laptop asset stolen from a vehicle	• Employee admitted report was a lie ... threw the computer out apartment window … where it was swept up and put in compactor and crushed • On business travel to South Africa • Employee had lunch at approx. 11am PDT. This was last place employee remembers seeing company iPhone until prepared for bed at approx. 9pm

- **CI training of work force**
  - Foreign threat at work (CONUS and OCONOUS)
  - Insider threat

Agenda

- DoD efforts to safeguard Controlled Technical Information (CTI)
- Tailored engagements
- Tunable Response Options
- **Defense Industrial Base (DIB)'s role in the process**

DIB Role

- **Identify crucial elements for protection up front**
  - Requires coupling technical know how with CI/LE expertise
- **Report**
  - Cyber incidents
  - Suspicious contacts
- **Consider joining the DIB CS program:**
  - Enables Government to Industry information sharing
  - Apply to the DIB CS program at http://dibnet.dod.mil/
- **Maintain an open dialogue with all the protection stakeholders**
  - Counterintelligence, Law Enforcement, Network Security, etc.

The DIB is a critical partner in preventing unauthorized access to precious U.S. intellectual property and manufacturing capability by adversaries

Questions

Mr. Brian D. Hughes

Director, Joint Acquisition Protection and Exploitation Cell (JAPEC)

brian.d.hughes3.civ@mail.mil

571-372-6451