Protecting US Military's Technical Advantage: *Assessing the Impact of Compromised Unclassified Controlled Technical Information*

Mr. Brian D. Hughes

Office of the Deputy Assistant Secretary of Defense for Systems Engineering

18th Annual NDIA Systems Engineering Conference

Springfield, VA | October 28, 2015

Distribution Statement A – Approved for public release by DOPSR on 10/21/2015, SR Case # 16-S-0130 applies. Distribution is unlimited.

These are Not Cooperative R&D Efforts

U.S. HUMVEE

China's
Dongfeng EQ2050

U.S. Reaper

China's Yìlóng-1

Agenda

- **DoD efforts to safeguard Controlled Technical Information (CTI)**
- **Evolving DoD policy to evaluate the compromise of CTI**
- **DoD cyber intrusion damage assessment process**
- **Defense Industrial Base (DIB)'s role in the process**

Distribution Statement A – Approved for public release by DOPSR on 10/21/2015, SR Case # 16-S-0130 applies. Distribution is unlimited.

Agenda

- **DoD efforts to safeguard Controlled Technical Information (CTI)**
- **Evolving DoD policy to evaluate the compromise of CTI**
- **DoD cyber intrusion damage assessment process**
- **Defense Industrial Base (DIB)'s role in the process**

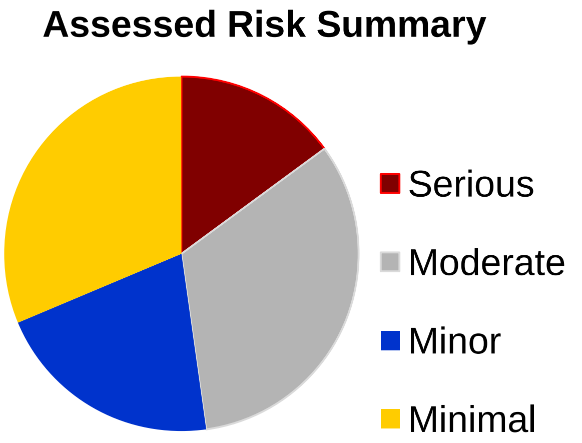
Significant DoD Losses

Bulk of DoD technical data resides on unclassified non-DoD networks

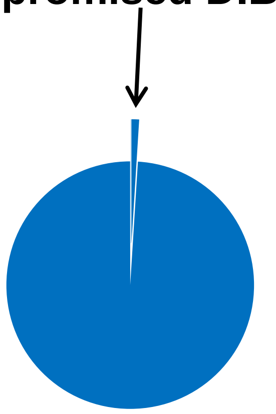
– As we moved to a world where data is both developed and conveyed electronically, traditional physical security concepts and constructs are no longer valid

DIB CS/IA DAMAGE ASSESSMENT NOMINATIONS

- *More than 10% assessed as serious*



DoD has only assessed a small amount of the compromised DIB data



DIB Network Technical Data Exfiltration

Cyber is not the only exploit….

- Joint Ventures
- Export Violations
- Insider Threats
- Academic Exchanges
- Others

Requires an all source look to fully comprehend the impact

DoD Efforts to Address DIB Cyber Intrusions

- **In 2007 DoD launched the Defense Industrial Base Cybersecurity/Information Assurance (DIB CS/IA) program**
  - Voluntary program enables Government-Industry threat information sharing, industry cyber incident reporting, and damage assessment of information losses
  - Currently 128 partners and ~125,000 threat information products shared
  - DIB Enhanced Cybersecurity Services (DECS) provides additional engagement with commercial service providers
- **DFARS 252.204-7012 published Nov 18, 2013 requires mandatory reporting of compromised Unclassified Controlled Technical Information**
  - Required reporting within 72 hours of discovery of any reportable cyber incident
  - Reportable cyber incidents include:
    - A cyber incident involving possible exfiltration, manipulation, or other loss or compromise of any unclassified controlled technical information resident on or transiting through Contractor's, or its subcontractors', unclassified information systems.
- **DFARS 252.204-7012 updated with interim rule on August 26, 2015 to address safeguarding of Covered defense INFORMATION**
  - Covered defense INFORMATION includes
    - Controlled Technical Information
    - *Critical information (operations security)*
    - *Export control*
  - Enables submission of the malicious software associated with the cyber incident to DoD (if the contractor discovers and is able to isolate)
  - Does NOT enable Government - Industry threat information sharing

Agenda

- DoD efforts to safeguard Controlled Technical Information (CTI)
- **Evolving DoD policy to evaluate the compromise of CTI**
- DoD cyber intrusion damage assessment process
- Defense Industrial Base (DIB)'s role in the process

Distribution Statement A – Approved for public release by DOPSR on 10/21/2015, SR Case # 16-S-0130 applies. Distribution is unlimited.

Addressing the Loss of CTI

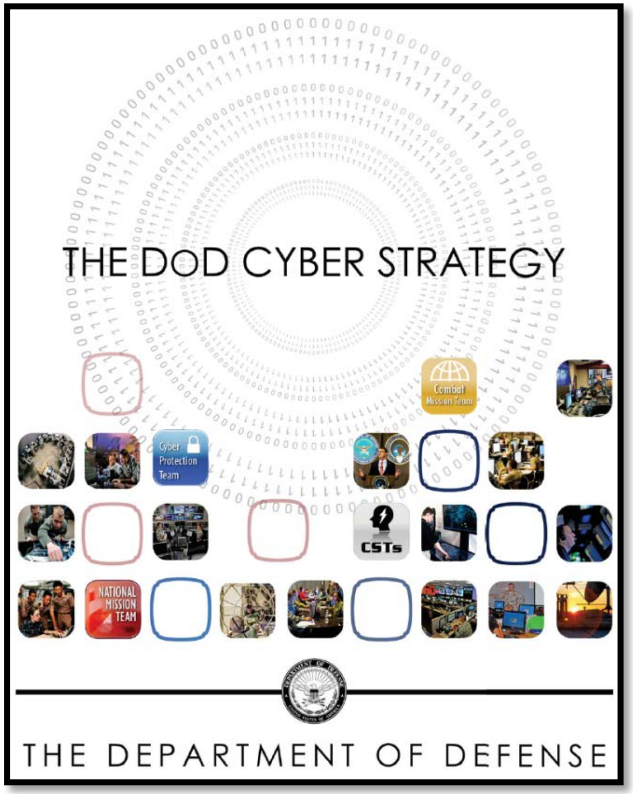
Risk = f (threat, vulnerabilities, consequences)

Goals:

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

Distribution Statement A – Approved for public release by DOPSR on 10/21/2015, SR Case # 16-S-0130 applies. Distribution is unlimited.

DoD Policy



- **Cyber: Defense Cyber Strategy, April 23, 2015:**
  - "DoD will establish a Joint Acquisition Protection and Exploitation Cell (JAPEC)…"
  - DoD will conduct comprehensive risk and damage assessments of cyber espionage and theft to inform requirements, acquisition, programmatic, and counterintelligence courses of action.
- **Acquisition: Better Buying Power 3.0, April 9, 2015**
- **Intelligence: Consolidated Intelligence Guidance (FY17-21), June 6, 2015**
  - Planning and Programming Guidance for the National Intelligence Program and the Military Intelligence Program

"ASD(R&E) and the Services, with USD(I), Defense Security Service (DSS), CIO, and DIA will develop and demonstrate a process to link counterintelligence, law enforcement, and acquisition activities by establishing a joint analysis capability to improve enterprise protection of classified and unclassified technical information."

-- USD(AT&L), BBP 3.0 Implementation Instructions, April 9, 2015

Distribution Statement A – Approved for public release by DOPSR on 10/21/2015, SR Case # 16-S-0130 applies. Distribution is unlimited.

JAPEC Mission: Integrated Analysis

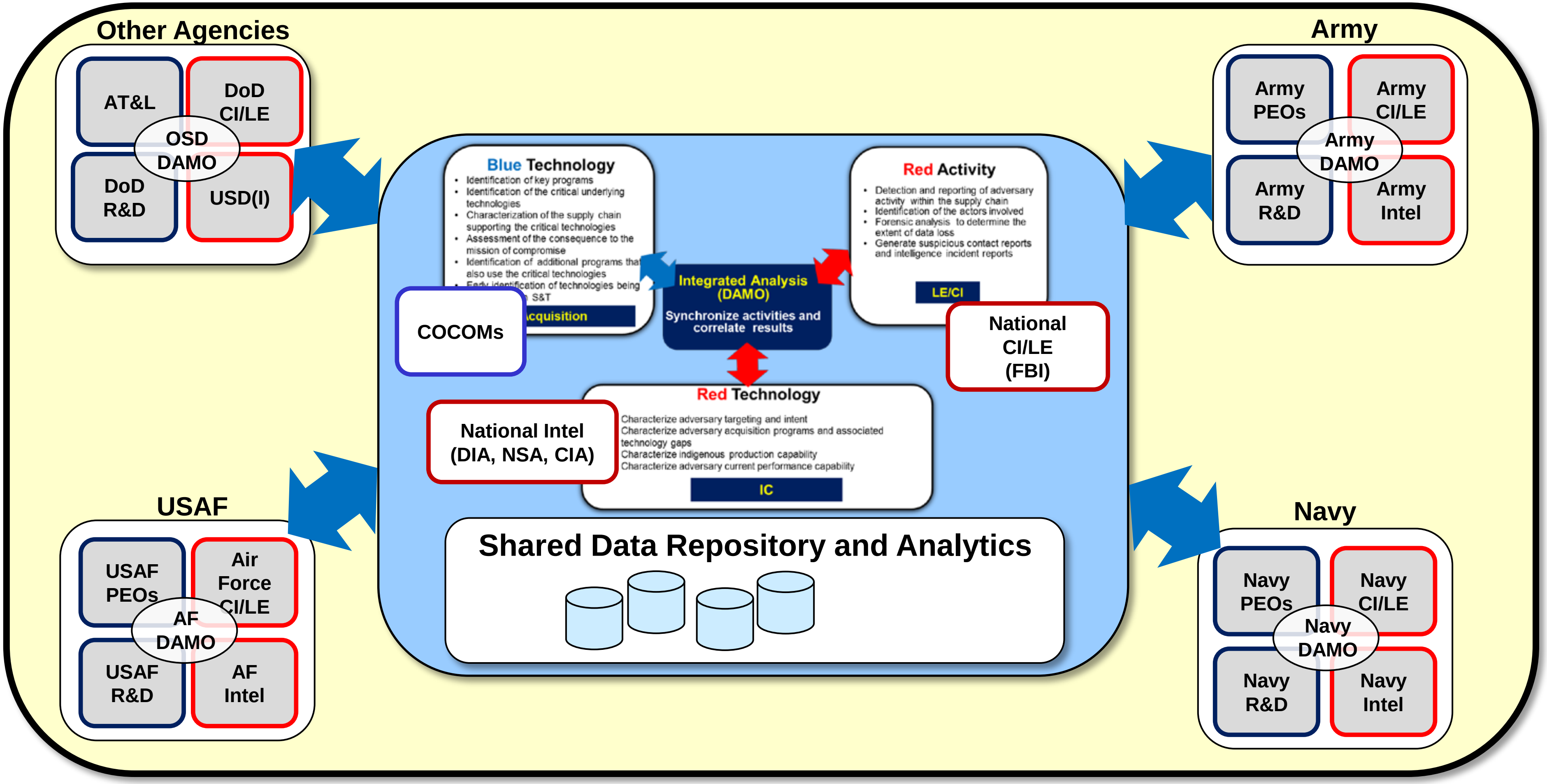
The Joint Acquisition and Protection Cell (JAPEC) integrates and coordinates analysis to enable Controlled Technology Information (CTI) protection efforts across the DoD enterprise to proactively mitigate future losses, and exploit opportunities to deter, deny, and disrupt adversaries that may threaten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

U.S. AIR FORCE

Capabilities Management Office (CMO)

JAPEC: Integrating Analysis Done at the Enterprise-Level

JAPEC



Blue Technology

- Identification of key programs
- Identification of the critical underlying technologies
- Characterization of the supply chain supporting the critical technologies
- Assessment of the consequence to the mission of compromise
- Identification of additional programs that also use the critical technologies
- Early identification of technologies being [illegible] S&T

Red Activity

- Detection and reporting of adversary activity within the supply chain
- Identification of the actors involved
- Forensic analysis to determine the extent of data loss
- Generate suspicious contact reports and intelligence incident reports

Integrated Analysis (DAMO)

Synchronize activities and correlate results

Red Technology

Characterize adversary targeting and intent
Characterize adversary acquisition programs and associated technology gaps
Characterize indigenous production capability
Characterize adversary current performance capability

Damage Assessment Focus

- **Damage Assessment focuses on determining the impact of compromised CTI, NOT on the mechanism of cyber intrusion.**

  Does this information enable an adversary to:

  reverse engineer;
  counter; or
  defeat US capability?

  – Clone
  – Counter
  – Kill

- **Assessment not possible without access to compromised material:**
  – Addressed in regulatory activities

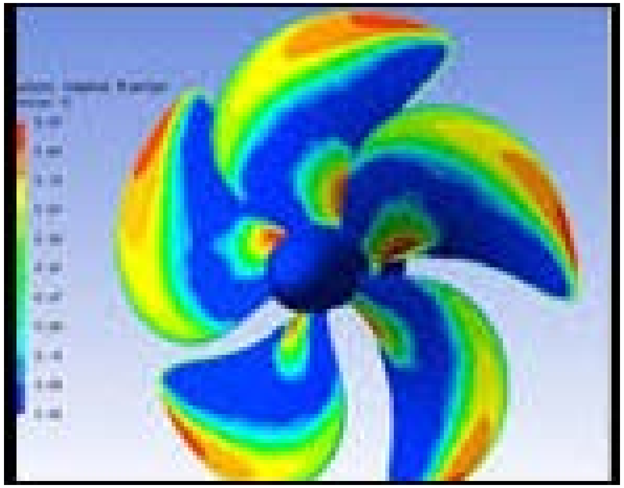
- **Purpose of resulting assessment:**
  – Trigger action across the linked communities (Acquisition, IC, CI, and LE)

Distribution Statement A – Approved for public release by DOPSR on 10/21/2015, SR Case # 16-S-0130 applies. Distribution is unlimited.

Case Study: Failure to Protect

USS Sturgeon Class

Soviet Victor III



Circumvention of protection schemes enabled parity

Tunable Response Options

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

Agenda

- DoD efforts to safeguard Controlled Technical Information (CTI)
- Evolving DoD policy to evaluate the compromise of CTI
- DoD cyber intrusion damage assessment process
- **Defense Industrial Base (DIB)'s role in the process**

Distribution Statement A – Approved for public release by DOPSR on 10/21/2015, SR Case # 16-S-0130 applies. Distribution is unlimited.

DIB Role

- **Ensure appropriate action when CTI compromise occurs:**
  - Communicate with your stakeholders (e.g. program office, security (physical, network), contracts)
- **Provide compromised data to the DoD in an expeditious manner**
  - Compromise is not the same as Exfiltration
- **Work with DoD to recommend alternate protection measures**
- **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 by adversaries

Distribution Statement A – Approved for public release by DOPSR on 10/21/2015, SR Case # 16-S-0130 applies. Distribution is unlimited.

Questions

Mr. Brian D. Hughes

Director, Joint Acquisition Protection and Exploitation Cell (JAPEC)

brian.d.hughes3.civ@mail.mil

571-372-6451

Distribution Statement A – Approved for public release by DOPSR on 10/21/2015, SR Case # 16-S-0130 applies. Distribution is unlimited.