



**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**

Cybersecurity for Advanced Manufacturing Conference
August 18, 2016



Case Study: Failure to Protect



USS Sturgeon Class



Soviet Victor III

Insider Threat: Walker Spy Ring (1967-1985) enabled Soviets to decipher U.S. military radio messages identifying Soviet acoustic vulnerability.

Soviet Fast Attack Production

Victor I – IOC 1967
16 produced

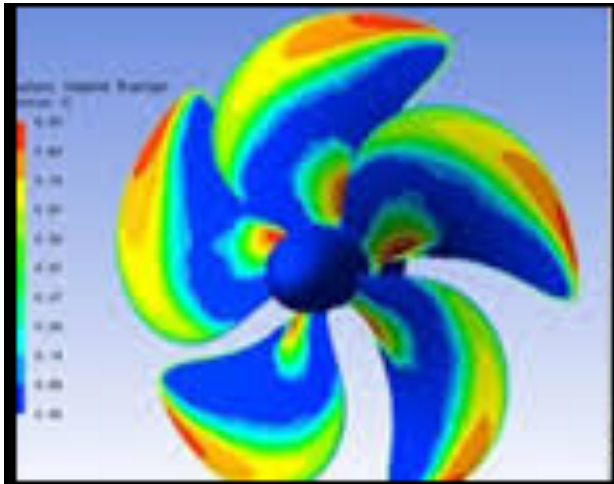
Victor II – IOC 1972
7 produced

Victor III – IOC 1979
25 produced

Insider peeled away first layer of protection



Obtaining the Technology



- **In 1981 Soviets obtained propeller milling machines and numerical controllers:**
 - Sales involved export control violations

Circumvention of non military technology protection schemes closed the gap



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

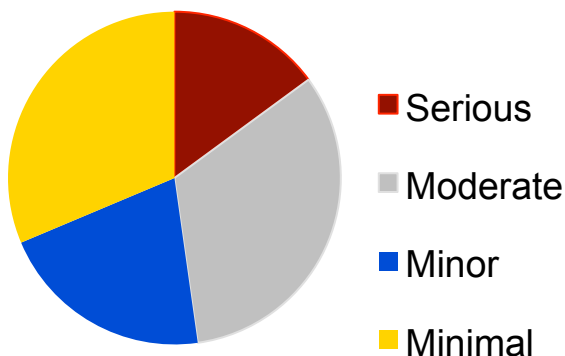
Bulk of DoD technical data resides on unclassified non-DoD networks

- As we moved to a world where data is both developed and conveyed electronically, traditional physical security concepts and constructs are no longer valid.
- Merging data with manufacturing compounds the problem.

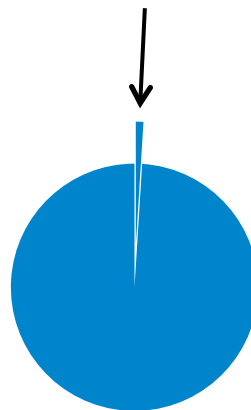
DIB CS/IA DAMAGE ASSESSMENT NOMINATIONS

- *More than 10% assessed as serious*

Assessed Risk Summary



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 155 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 (Network Penetration Reporting and Contracting for Cloud Services) on August 26, 2015 to address safeguarding of Covered Defense Information (CDI). CDI 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



Addressing the Loss of CTI

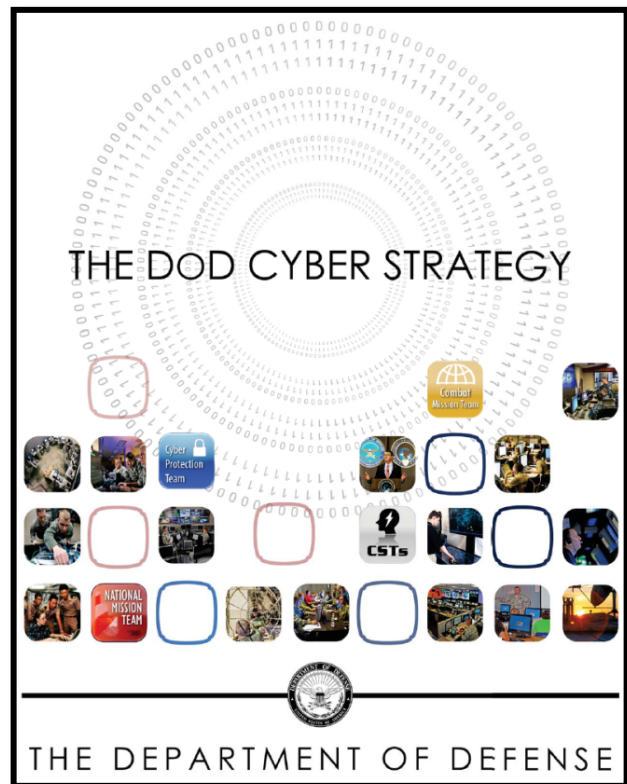
$$\text{Risk} = f(\text{threat, vulnerabilities, consequences})$$

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**



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



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.

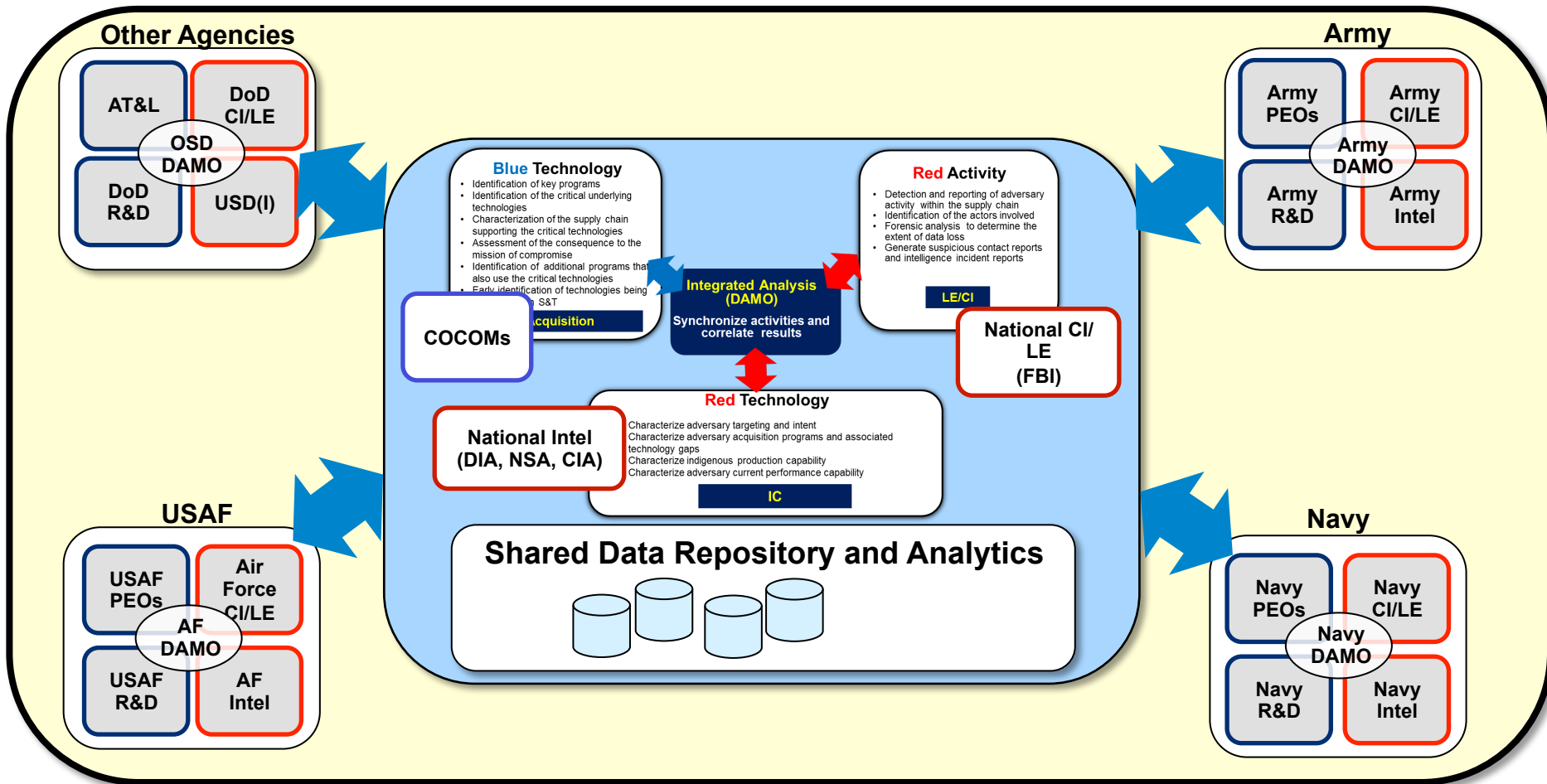




JAPREC: Integrating Analysis done at the Enterprise-Level



JAPREC





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)



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



Damage Assessment Focus

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

Does this information enable an adversary to:
reverse engineer;
counter; or
defeat US capability?
- **Assessment not possible without access to compromised material:**
 - Addressed in regulatory activities
- **Purpose of resulting assessment:**
 - Trigger action across the linked communities (CI, LE, IC and Acquisition)



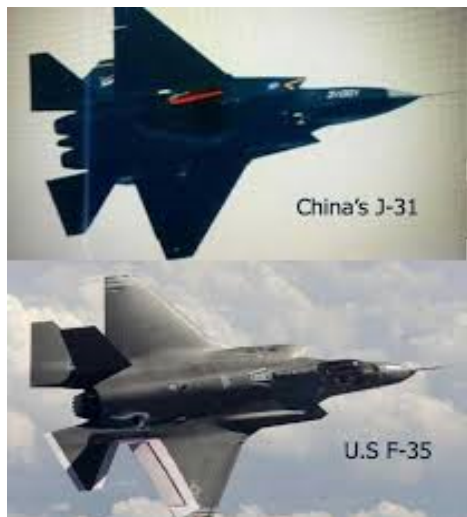
Agenda



- 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**



These are NOT Cooperative R&D or Joint Manufacturing Efforts



China's J-31

U.S. F-35



Russia's A-50



U.S. E-3C



U.S. HUMVEE



China's
Dongfeng EQ2050



U.S. Reaper



China's Yìlóng-1



DIB Role

- **Incorporate protection to advanced manufacturing capability up front:**
 - Compromise will be much more serious than information alone
- **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 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