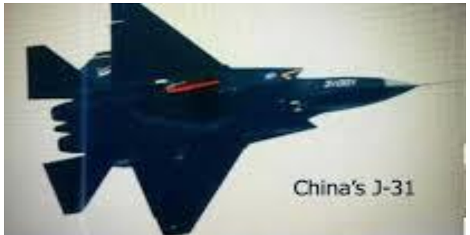
Engaging the DoD Enterprise to Protect U.S. Military Technology Advantage

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

20th Annual NDIA Systems Engineering Conference
Springfield, VA | October 25, 2017

These are Not Cooperative R&D Efforts



China's J-31

U.S F-35

KJ-2000

E-3C

M-16

QBZ-95

HUMVEE

Dongfeng EQ2050

Reaper

Yìlóng-1

Case History: Titanium Dioxide

Walter Liew, a naturalized American citizen, business owner, and technology consultant stole DuPont's protocols for producing its superior titanium white from 1997 through 2011

- DuPont developed $2.6B per annum Titanium Dioxide business – recognized as world leader
  - Processes created in 1940s but spent $150M year to improve processes by 1%
    - Near monopoly on the manufacturing techniques
  - Shielded its titanium dioxide process
    - Guards
    - Escorted Visitors
    - Documents and blueprints controlled
  - Starting in 1990's China began seeking ways to illegally acquire DuPont's methods
    - China accounts for approximately 25% of the demand

Liew was convicted in 2014 on each of twenty counts with which he was charged and sentenced to serve 15 years in prison, forfeit $27.8 million in illegal profits, and pay $511,667.82 in restitution

Bottom Line Up Front

- **Adversary is targeting our Controlled Technical Information (CTI)**
- **DoD is emphasizing protection activities to encompass the full range of threats and vulnerabilities across the acquisition life cycle**
- **The Joint Acquisition and Protection and Exploitation Cell (JAPEC) enables a comprehensive analysis of protections for DoD's critical programs and technologies (CP&T) and addresses shortfalls**
- **Significant amount of technical expertise resides in the Defense Industrial Base (DIB)**
- **The DIB is not only critical to protecting that information but helping DoD identify which information it should protect**

Partnership between DoD and DIB is vital

Agenda

- **DoD Efforts to Safeguard Controlled Technical Information (CTI)**
- **Know the Environment**
- **Stakeholder Dialogue**
- **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, Law Enforcement (LE), Counterintelligence (CI), and Intelligence Community (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 and Exploitation 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.

Identifying Critical Programs and Technologies for Proactive Protection

ACQUISITION
- Identify DoD's Critical Acquisition and Technology
- Link technologies across the enterprise
- Identify protection methods
- Educate the workforce

SECURITY
- Integrate CI/Security posture
- Coordinated Security Classification Guides
- Onsite protection at DIB
- Contractor threat education

COUNTERINTELLIGENCE/ LAW ENFORCEMENT
- Collect against adversary activity
- Field presence
- Facility security analysis
- CI threat assessment
- Investigations & Prosecution

Program Technology Capability Selection

Access to Supply-chain Channels

Define Key *Areas and Avenues of Risk*

EVALUATE
- Impact of Compromise
- Areas of Vulnerability
- Exploitation

Develop Coordinated Mitigation Program

REQUIREMENTS
- Revise requirements based on change in threat

INTELLIGENCE
- Identify adversary technologies needs

DIB
- Understand Supply Chain
- Proactive approaches
- Improve Information Sharing w/ DoD

CIO/NETWORK SECURITY
- Tiered IT security controls
- Enroll in threat sharing forums

JAPEC projects demonstrated the effectiveness of an integrated iterative approach. JAPEC methods complement other DoD efforts.

Agenda

- DoD Efforts to Safeguard Controlled Technical Information (CTI)
- **Know the Environment**
- Stakeholder Dialogue
- Defense Industrial Base (DIB)'s Role in the Process

Understanding Your Supply Chain

- **Increase level of concern for DoD's protection priorities throughout the supply chain**
  - Includes vendors, mergers, acquisitions, subsidiaries
- **Executive Order on Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States dtd 21 July 2017**
- **Within 270 days**
  - (a) identifies military and civilian materiel, raw materials, and other goods essential to national security;
  - (b) identifies manufacturing capabilities essential to producing goods identified pursuant to subsection (a) of this section, including emerging capabilities;
  - (c) identifies defense, intelligence, homeland, economic, natural, geopolitical, or other contingencies that may disrupt, strain, compromise, or eliminate supply chains of goods identified pursuant to subsection (a) of this section (including as a result of the elimination of, or failure to develop domestically, capabilities identified pursuant to subsection (b) of this section) and that are sufficiently likely to arise so as to require reasonable preparation for their occurrence;
  - (d) assesses resiliency and capacity of manufacturing and defense industrial base and supply chains of the United States to support national security needs

How well do you know your supply chain?

Agenda

- DoD Efforts to Safeguard Controlled Technical Information (CTI)
- Know the Environment
- **Stakeholder Dialogue**
- Defense Industrial Base (DIB)'s Role in the Process

Dialogue with Protection Stakeholders

- **Compliance with existing rules & 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 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
- **DoD/DIB information sharing improves the US' ability to focus priorities on most critical technologies**
  - Timely reporting to DoD which includes more than cyber incidents
  - Information sharing forums enable you to learn from other's experiences

Adversary is Dynamic and Active

Agenda

- DoD Efforts to Safeguard Controlled Technical Information (CTI)
- Know the Environment
- Stakeholder Dialogue
- **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
  - Develop and implement training that focuses specifically on CTI handling and protection requirements
- **Do you have your own list of technologies crucial to you?**
- **Report**
  - Cyber incidents
  - Suspicious contacts
  - Media Theft and Loss
  - Insider Threats
- **Consider joining the DIB CS program**
  - Enables Government to Industry information sharing
  - Join and contribute to the DIB CS program at http://dibnet.dod.mil/
  - Share cyber forensic reports with DoD
- **Maintain an open dialogue with all the protection stakeholders**
  - Counterintelligence, Law Enforcement, Network Security, etc.
  - Targeting U.S. Technologies: A Trend Analysis of Cleared Industry Reporting at http://www.dss.mil/documents/ci/2017_CI_Trends_Report.pdf

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

Systems Engineering: Critical to Defense Acquisition










Defense Innovation Marketplace
http://www.defenseinnovationmarketplace.mil

DASD, Systems Engineering
http://www.acq.osd.mil/se

Questions

Mr. Brian D. Hughes

Director, Joint Acquisition Protection and Exploitation Cell (JAPEC)

brian.d.hughes3.civ@mail.mil

571-372-6451