HELLO, MOSCOW. GREETINGS, BEIJING. ADDRESSING RISK IN YOUR IT SUPPLY CHAIN

MODERATOR: Edward Brindley
Principal Deputy, DCIO/CS in DoD-CIO

Mr. Don Davidson
Deputy Director, Cyber Security Risk Management, US DOD-CIO

PANELISTS: Mr. Emile Monette
Cybersecurity Strategist, Department of Homeland Security (DHS)

Mr. Jon Boyens
Manager, Security Engineering & Risk Management, National Institute of Standards and Technology (NIST)

Ms. Angela Smith
Sr Advisor for Cybersecurity, Risk, and Resilience, General Services Administration (GSA)
SUPPLY CHAIN RISK: AN OVERVIEW
Supply Chain: PERSPECTIVES - Product Integrity/Software Assurance and Hardware Assurance (Anti-Counterfeit)

How do we improve our trust & confidence from a global ICT supply chain?

IT and Communications products are assembled, built, and transported by multiple vendors around the world.

Software contributions include reusable libraries, custom code, commercial products, open source

One telecom provider Looked at software (84 different first tier suppliers for the software)
"This is a trend the department has frankly been willing to recognize more in policy than in practice...I'd hazard a guess that 25 years ago, 70 percent of the goods and services the department procured were developed and produced exclusively for the military. Today, that ratio has reversed. Seventy percent of our goods and services are now either produced for commercial consumption or with commercial applications in mind. And it’s backed by a largely commercial-based supply chain."

– Mr Brett Lambert, former DASD for Manufacturing and Industrial Base Policy
Existing and Emerging Research, Policy, Standards and Practices

**Government**
- Software & Supply Chain Assurance (SSCA) Forum (Public-Private Partnership)
- CNCI Stood Up
- DoD ICT SCRM Key Practices
- PMOs developed in DOJ, DOE and DOC
- UMD Research
- Industry Best Practices
- NIST IR 7622
- Sec 515/516 for CJS
- Cybersecurity Framework
- And Roadmap
- GAO Report
- NIST SP 800-800-161
- NIST SP 800-171
- CNSSD 505 Update


**Industry**
- SAFECODE Software Supply Chain Integrity papers
- Common Criteria Supply Chain Security Assurance
- Open Trusted Technology Standard ISO/IEC 20243
- IEC 62443-2-4 – Industrial-process measurement, control and automation
- Risk Analytics
- ISO/IEC 27036 – Information Security in Supplier Relationships
- SAFECode Use of Third Party Components
- ABA Vendor Checklist
- In Contracts

**2016 2017**
- OMB Circular A-130 Metrics White Paper
- China TC260: GB C-SCRM Standard
- Draft NIST IR 8179 Criticality Analysis

**Draft CSF v1.1**

**NIST SP 800-171**
Risk Management Framework (RMF) & Supply Chain Risk Management (SCRM)

All-Source Intelligence

Commercial Due Diligence
Open-Source Business Information

Better use of commercial standards

DODI 5200.44 TSN
CNSSD 505 SCRM
NIST SP 800-161 SCRM
Supply Chain Risk Management (SCRM) Working Groups (WGs)

US has vital interest in the global supply chain.

SCRM believes “commercially acceptable global standard(s)” must be derived from Commercial Industry Best Practices.

SCRM Standardization Requires Public-Private Collaborative Effort
SUPPLY CHAIN RISK: IN THE NEWS
Kaspersky Labs/ DHS Issued Binding Operational Directive (BOD) 17-01 on September 13, 2017

- **BOD calls on Departments and Agencies to:**
  - Identify any use or presence of Kaspersky products on their information system.
  - Implement plans to discontinue use and remove the products from information systems.

- **Rationale for BOD:**
  - Kaspersky products present information security risks to federal information systems.
  - Anti-virus products and solutions provide broad access to files and elevated privileges on the computers on which the software is installed, which can be exploited by malicious cyber actors to compromise those information systems.

*Source: DHS BOD 17-01*  
A Case Study: BLU Phone


  - Preinstalled software on BLU R1 HD transmitted the full contents of text messages, contact lists, call logs, location information and other data to a Chinese server.
  - Code developed by Chinese company Shanghai Adups Technology Company, which runs on more than 700 million phones, cars and other smart devices.
  - Demonstrates “how companies throughout the technology supply chain can compromise privacy, with or without the knowledge of manufacturers or customers.”

SUPPLY CHAIN RISK: TAKING IT HOME
Applying Supply Chain Risk Management

Awareness + Action = Organizational Risk Mitigation

**Awareness** of cyber SCRM risk, threats, and vulnerabilities within your organization and supply chain.

Development of organizational cyber **SCRM plans**, training and awareness efforts, execution of business due diligence, or inclusion of SCRM-specific contract clauses.

**Reduction of overall risk** from cyber supply chain threats.
Cyber Supply Chain Risk Mitigation Within Your Organization

- Next week / ASAP you should:
  - Assess and identify cyber supply chain risk practices within your organization.
  - Become familiar with SCRM best practices (ex: NIST 800-53).

- In the first three months following this presentation you should:
  - Identify gaps within organizational supply chain practices and potential steps for remediation.
  - Ex: Need for organizational SCRM plan, training and awareness efforts, etc.

- Within six months you should:
  - Begin to implement changes.