Cyber Supply Chain Risk Management: Identifying & Mitigating Threats to the IC

Breakout Session

Overview

The Intelligence Community (IC), like most enterprises in today's interconnected world, depends upon a complex and global supply chain to obtain the goods and services it needs. The insertion of malicious code or vulnerable hardware in the IC's information and communications technology (ICT) supply chain threatens national security as adversaries could steal intellectual property, access sensitive communications, or modify system operation. The IC is committed to partnering with industry to manage supply chain risk by identifying both trusted vendors and threats.

Summary

This panel discussed the IC's efforts to illuminate its supply chains and better train its cybersecurity personnel. New agencies and certifications promise to tighten the focus on risk management, but further collaboration is needed with industry.

Panelists

- **Katie Arrington,** Chief Information Security Officer (CISO), Office of the Assistant Secretary of Defense for Acquisition (OUSD(A))
- **Bob Kolasky,** Director, National Risk Management Center, Department of Homeland Security
- **Scott Rush**, Deputy CISO, Lockheed Martin
- **Bill Stephens,** Director for Counterintelligence, Defense Counterintelligence and Security Agency
- **Harvey Rishikof,** Professor, Temple University Beasley School of Law (moderator)

Key Takeaways:

- Software, hardware, people and information are the four main aspects of any supply chain. Each has to be secured in a different manner.
- The Cybersecurity Maturity Model Certification (CMMC), developed by the OUSD(A), will soon be required for every company within the DoD supply chain. A company must score a maturity level 3, which is equivalent to NIST 800-171 compliance. The CMMC is set to go live in June 2020.
- The National Risk Management Center, part of the new Cybersecurity and Infrastructure Security Agency (CISA), has been examining strategic risks to the federal network and the 16 critical infrastructure sectors. Its assessment has been delivered to the Secretary of Commerce.
- The National Background Investigations Bureau (NBIB) will merge into the Defense Counterintelligence and Security Agency (DCSA) on October 1, transferring responsibility for performing background checks of potential contractors in supply chains from OPM to DoD.
- Rapid 5G network speeds create an exposure space that is unprecedentedly large – a breach of an organization's network could lead to the exfiltration of terabytes of data in mere seconds. However, there is still time to include security into 5G evolution and standards. Trusted vendor material is important.
- DoD 5000 is being condensed from 3,000 pages to 7. The revised version, which is set to be released in December, will teach project managers (PM) to think about cybersecurity holistically. Too often, PMs are certified but not fully qualified for their jobs.

Recommendations

- Read MITRE's report, "Deliver Uncompromised."
- Government should help small businesses transition to the cloud to increase their CMMC scores. Small businesses are the baseline of innovation, and the DoD should strive to include them.
- Decrease bureaucracy so that federal employees can work for government, transition to industry to gain critical skills, then return to government.
- Connect industry with decision makers in government to build security protocols into 5G standards and evolution.
- Ensure that non-cyber supply chain components are secured - for example by vetting the people working on critical hardware, software, and related components to prevent threats of theft or sabotage from trusted insiders.

ABOUT INSA

The Intelligence and National Security Alliance (INSA) is the leading nonpartisan, nonprofit trade association for driving public-private partnerships to advance intelligence and national security priorities. A 501(c)(6) membership organization, INSA strives to identify, develop, and promote collaborative approaches to national security challenges. INSA has more than 160 organizations in its membership and enjoys extensive participation from leaders and senior executives in the public, private, and academic sectors. Learn more at www.INSAonline.org.