Counterintelligence Support to Supply Chain

FISWG

October 28, 2020

Douglas Thomas

Director, Counterintelligence Operations & Corporate Investigations

Introduction & Background

- Douglas D. Thomas – Director, Lockheed Martin Counterintelligence Operations & Corporate Investigations (COCI)
  - 33 Years With The Air Force Office Of Special Investigations (AFOSI); Retired As Executive Director
  - 2 Years As The Principle Deputy Director Of The National Counterintelligence Executive (NCIX)

COCI Mission Spectrum

Counterintelligence

- Insider Threat Program
- Insider Threat Detection/ Continuous Evaluation
- ITPSO/NISPOM Change 2
- CI Support to Supply Chain
- Middle Way
- University Engagement
- CI Investigations
- Suspicious Contact Reporting
- Air & Tradeshow Support
- OSINT
- Training & Awareness

Investigations

- Centralized Investigations Team: Corporate-Wide
- Workplace Violence Prevention & Response
- Investigations 101 Training
- Threat Management Team Training

Problem Set for Industry

- Theft of technology
  - Loss of revenue (future & current)
- Counterfeiting
  - Potential for sub-par components and lawsuits
- Sabotage
  - Potential to insert components which may be designed to fail or malfunction immediately or at some point in the future
- Acquisition of program/system intelligence
  - Sensitive program information could potentially yield engineering of defense & weaponry countermeasures
  - System limitation information could allow for engineering of offensive measures
- Severe damage to reputation

"The theft of intellectual property by foreign countries costs our Nation millions of jobs and billions and billions of dollars each and every year."

President Donald Trump, 2017

Expanding Opportunities for Compromise

- Cyber intrusions on corporate and/or unwitting suppliers' systems
- Co-opted suppliers
- Traditional insider threat recruitment
- Partnerships with criminal enterprises or adoption of their methods
- Foreign government control over foreign suppliers
- Development of front companies (CONUS and OCONUS)
- Exploitation of Mergers & Acquisitions

"We cannot afford a situation five years from now where we may spend a lot of money building a thing, and then we need that thing to defend our nation, and it's been compromised via supply chain and it doesn't work"

Bill Evanina, Director, National CI & Security Center, 2019

Recent Government Actions

- Deliver Uncompromised Report – 8 August 2018
- SecDef Mattis Memo – 24 October 2018
  - Protecting Critical Technology Task Force
- Maj Gen Murphy Memo – 17 June 2019
  - *Integrating and Elevating Security in the Acquisition Process*
- Updated Implementation of "The DIB" Memo – 6 September 2019
  - Safeguarding Covered Defense Information and Cyber Incident Reporting
- USD(R&E) Griffin Memo – 10 October 2019
  - DoD and University Partnerships
- National Defense Authorization Act (NDAA) – FY2019
  - Prohibition on certain video surveillance/telecommunications equipment
- Bureau of Industry & Security (Dept. of Commerce) Entity List Updates – 2020
- National CI Strategy – 10 February 2020
  - *Reduce Threats to Key U.S. Supply Chains*

"The [DOD] does not take security sufficiently into account when determining which partners to partner with, nor is security adequately considered in program evaluations"

MajGen Murphy, Director, Protecting Critical Technology Task Force, 2019

USD(A&S) DoD Directive Update

- DoD Directive 5000.01; The Defense Acquisition System
- Describes the principles governing the acquisition process; emphasizing main tenets of acquisition
- Update signed into effect by DepSecDef David L. Norquist – September 2020
- Mandates incorporation of CI requirements throughout technology/system/service lifecycle
- Section d - Develop and Deliver Secure Capabilities
  - *Security, cybersecurity, and protection of critical technologies at all phases of acquisition are the foundation for **uncompromised delivery** and sustainment of warfighting capability*
  - *Acquisition managers, in coordination with security and **counterintelligence** (CI) professionals, will implement initiatives and processes for the identification, integration and continual evaluation of security and CI requirements throughout the life cycle of a system, service, or critical technology*

"Deliver performance at the speed of relevance"

DoDD 5000.01

Lockheed Martin Actions

- Dedicated CI Support to Supply Chain Analyst
- CI Support to Supply Chain Strategic Plan
- Global Supply Chain Operations Risk Advisory Committee
- Software Vendor Screening
    - CI Support to other Supply Chain streams in progress
- Protecting the Middle Way
- University Engagement

"What has been established at Lockheed Martin is truly incredible and demonstrates the seriousness with which it protects technology through committed leadership, initiative, investment, and raw effort."

Daniel E. Payne, (Former)
Director, Defense CI & Security Agency, 2019

2019 Critical Technology Symposium

- Organized by Counterintelligence and Engineering & Technology Council
- Focused on two Critical Technologies
- 100 attendees including: VP of Engineering & Technology, LM Subject Matter Experts (SME), LM Security and Counterintelligence, FBI, CIA, DCSA, Air Force OSI
- USG presented on threats to critical technologies; LM SMEs briefed LM's future for those technologies
- Special guest provided insight into foreign intelligence activities
- Key Takeaways:
  - Adversaries are targeting next generation technologies at an accelerated and aggressive rate
  - More awareness of threats is required for LM SMEs
- (2020 Symposium postponed)

"All of the government presenters were fantastic, I really enjoyed the realism and examples they presented. Terrifying but really conveyed the importance of protecting our technologies.""

Critical Technology Symposium Attendee, 2019

Case Example

Questions?