Counterintelligence Support to Supply Chain

National Defense Industrial Association Supply Chain Summit

December 9, 2014

LOCKHEED MARTIN

Douglas D. Thomas
Director, Counterintelligence
Operations & Corporate Investigations

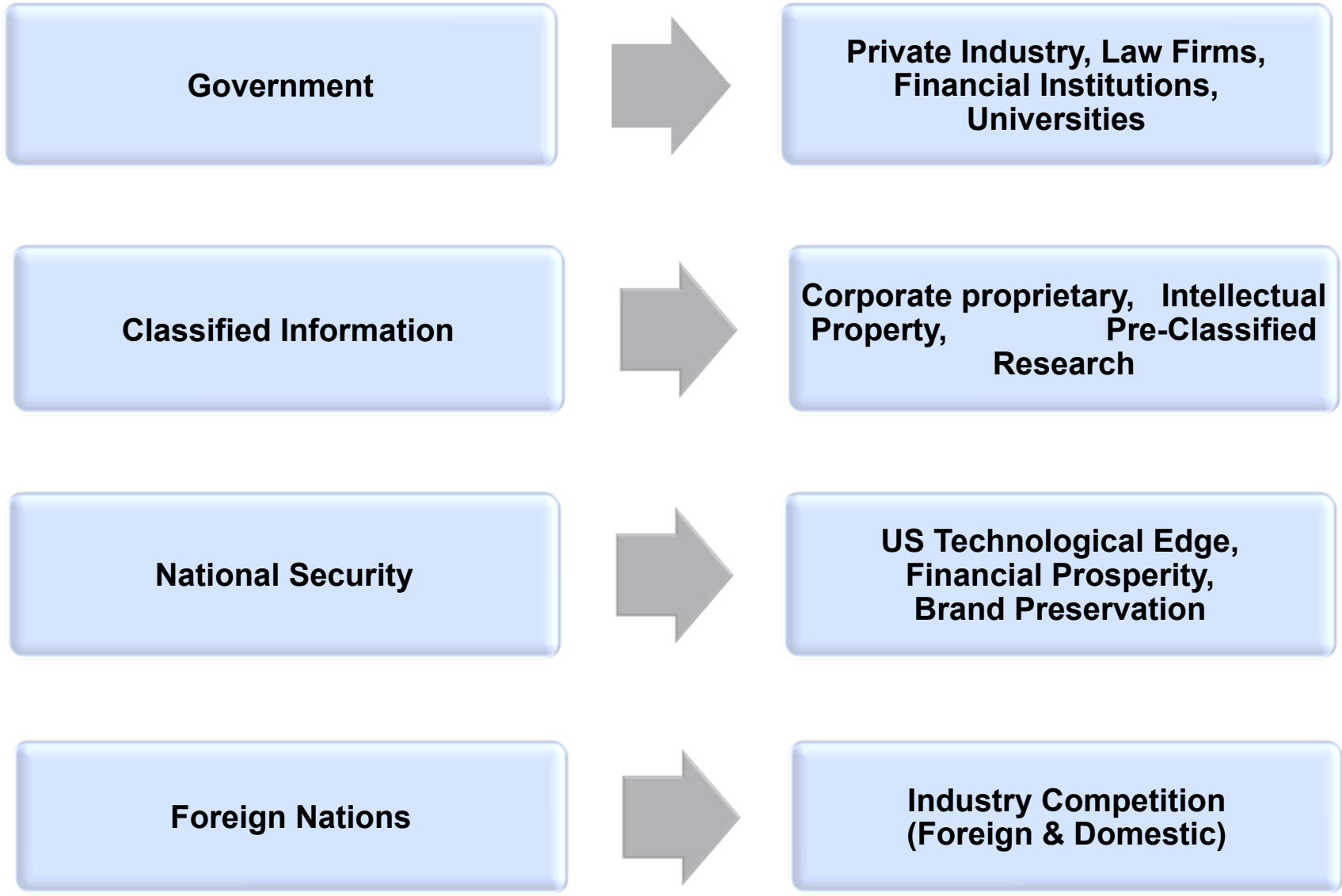
Introduction & Background

- **Douglas D. Thomas – Director, Lockheed Martin Counterintelligence Operations & Corporate Investigations**
  - **33 Years with the Air Force Office of Special Investigations; retired as Deputy Director**
  - **2 years appointed Deputy Director of the National Counterintelligence Executive**

Some Thoughts to Consider...

- **National Security is executed/funded by USG; *built* by Industry**
- **Government should have some assurances products & services are delivered uncompromised**
- **There is NO difference between National Security and Economic Security**
- ***MUST* think beyond classified programs and cleared people**
- **War Room → Board Room**
- **"Adversaries" in the government might be "business partners" in industry**

Perspective Change



Increase in Insider Threat

- The incidence of employee financial hardships during economic downturns
- The global economic crisis
  - Foreign nations more eager to acquire new technologies, R&D
  - Mergers, acquisitions, divestitures, joint ventures
- Ease of stealing anything stored electronically
- Increasing exposure to FIS presented by the reality of global business, joint ventures, and the growing international footprint of American firms.
- Increase in FIS recruitment of students

Government Response

- Appointment of US Intellectual Property Enforcement Coordinator
- Report to Congress on Foreign Economic Collection & Industrial Espionage
- Executive Order 13587
- Creation of the National Insider Threat Task Force
- Administration Strategy on Mitigating The Theft of Trade Secrets
- Anticipated NISPOM Conforming Change #2
- Insider Threat Language from the National Institute of Standards & Technology (NIST)
- CI Support to Contracts
- CI Support to Global Supply Chain Operations
- ICD 731, December 2013

LM Insider Threat Program

Planning

Selling Leadership
- Shifting landscape
- Trends
- Cost comparison
- Peer benchmarking

Peer Benchmarking
- Challenges/successes
- Population size
- Privacy considerations
- Program governance
- Budget
- Live analyst support

Review Committee
- HR, Legal, Privacy, Information Security, Communications, Ethics
- CONOPs
- Codification of Policy
- Communications Plan

Development

Tool Procurement / Development

Establish Potential Risk Indicators
- Determine appropriate weights and aging

Identification of Required Data Sets
- Agreements with data owners

Implementation

Data Ingestion and Tool Calibration

Roll-Out Message to Employees
- Transparency in objective
- Reinforcement of Leadership support
- Proper vehicles for voicing concern

Governance

Steering Committee
- Security, Legal, HR, Ethics, Information Security
- Receive Quarterly Briefings on Results
- Manage Policy Updates

Internal Audit

Board of Directors

LM WISDOM ITI™

- Evaluation of employee attributes, behaviors and actions according to analyst-defined models
- Lead generation and triage from three graphical outputs
- Automated link analysis
- Analyst defined categories and attributes of interest
- Categories and attributes are assigned weights
- Models run against an entire population or subsets
- Based on Big Data technologies (petabyte+)
- Notifications and alerts
- Data encryption

Threat to Supply Chain

- CI & Security issue with national attention
  - Director, NCIX, dubbed 2013 “Year of the Supply Chain”
  - National Counterintelligence Strategy lists “Assure the Supply Chain” as one of four strategic objectives
- Soft underbelly vulnerability
- Applicable to classified & unclassified technologies
- Very difficult to detect
- Vulnerabilities exist at all stages of the process
- Vendors are likely the softest target for exploitation
- Decision makers often focused solely on cost & schedule

Implications of Compromise

- Theft of technology
- 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

Developing Awareness of Threat

- **Supply Chain Vulnerabilities**
  - **While the threat and vulnerabilities are not new, they're largely ambiguous**
- **Still Developing:**
  - **Understanding of full scope of threat**
  - **Understanding of vulnerabilities**
  - **Understanding of effective measures for risk management**
- **Known challenges:**
  - **Expanding reliance on global resources**
  - **Accelerating trend towards multinational mergers**
  - **Detection capabilities likely outpaced by exploitation innovation**

Supply Chain - Challenges

- Challenges in identifying “key” components wrt intelligence threat
- Adversarial capabilities VERY difficult to quantify
- Little relevant/timely threat data from USG (methods, tactics, & targeting)
- USG reluctance to disseminate reporting on suspected front companies
- Exploitation innovation growing at an accelerated rate
- Global supply chain expansion continuously affords further opportunities for infiltration or exploitation
- If threat is not fully understood, vulnerability cannot be fully understood
- Growing offensive cyber capabilities have changed the game
- Complications with foreign government assistance
  - Intelligence threat = sanctioned/supported arm of foreign government
- Difficulties in attributing events
  - Terrorism or theft by criminal enterprise → immediate!
  - Intelligence compromise → ramifications may be significantly delayed

Methods for Intelligence Collection

- **Cyber intrusions on corporate systems and/or unwitting suppliers**
- **Co-opted suppliers**
- **Traditional Insider Threat methods**
- **Partnerships with criminal enterprises or adoption of their methods**
- **Governmental control over foreign suppliers**
- **Development of front companies (CONUS and OCONUS)**

Where's the Targeted Data?

- Procurement requisition information
- Contract specifications
- Design data
- Performance requirements
- Vendor identification (prime & sub-prime)
- Vendors' suppliers
- Shipment carriers
- Delivery schedules
- Installers & service providers
- Customers

Key Impact Questions

- How critical is the product?
  - What is its purpose?
  - Why is it important?
  - Is it a commodity or special purchase?
- Would an adversary be interested in exploiting it?
- How can it be touched?
- How exposed am I as the customer?
- What's the impact if compromised?
- What is the pedigree of my vendor?
- How will my vendor and I communicate?
- How is the vendor protecting my information?

Mitigation Recommendations

- Answer “Key Impact Questions”
- Consideration of CI Awareness Training requirement in contracts
- Use trusted US manufacturers, builders & installers where possible
- Diversity product selection when possible
- Continuously vet your vendors
- Stay apprised of vendor ownership changes
- Practice “need to know” with vendors
- Limit access to critical systems
- Educate yourself on how vendors protect your data on their networks
- Consistently use anti-tamper & tracking technology
- Pay close attention to shipping schedules

Mitigation Recommendations

- **Know who's touching your materials/shipments**
- **Periodically change procedures**
- **Educate your workforce & vendors on the importance of reporting suspicious anomalies**
- **Develop clear and detailed incident response procedures**
- **Investigate suspicious anomalies**
- **Maintain an incident tracking repository for analysis of historical data**
- **Supplier site visits by CI personnel for CI Awareness Training assessment**
- **Open source (OSINT) deep dive review on supplier portfolio**
- ***KNOW YOUR SUPPLY CHAIN!!***

Primary Takeaways

- Corporate proprietary information and intellectual property → hot targets
- Reporting indicates steady upward trend in targeting
- Threat is real, formidable and aggressive
- Current business environment exposes us to more vulnerabilities
- Strong partnerships are key (internal and external)
- Automated analysis capability is essential for any large organization
- Data Loss Prevention Tool ≠ Insider Threat detection capability
- Program transparency → mitigate concern and promote deterrence

Questions?