LOCKHEED MARTIN

100 YEARS OF ACCELERATING TOMORROW

SUPPLY CHAIN MANAGEMENT RISKS AND AWARENESS

IDENTIFY
MITIGATE
PRESERVE

Lockheed Martin's Office of Counterintelligence Operations identifies adversaries attempting to commit espionage by the gathering of information about our Corporation, our personnel, and/or our customers, and uses mitigation strategies to neutralize such threats. Success means collaborating with corporate security teams, counterintelligence leads and other functional organizations. We are focused on ensuring our reputation, customer/shareholder confidence, and a competitive edge for the benefit of our nation and its allies.

"Our supply chain is critical to ensuring Lockheed Martin can continue solving our customer's most difficult problems. Lockheed Martin Security and the Office of Counterintelligence Operations each are committed to ensuring you have the information you need to safeguard our employees, assets and information." — Bob Trono, Industrial Security Vice President, Lockheed Martin Corporation

HOW YOU CAN HELP PROTECT INFORMATION

As U.S. businesses continue expanding the reach of their products and services, security risks associated with foreign intelligence services also increases. Specifically, the globalization of today's economy has forced businesses such as Lockheed Martin to rely heavily on the global supply chain, which is an area with rapidly increasing vulnerabilities to intelligence threats.

SO WHAT DOES THIS MEAN FOR YOU?

Very simply, our adversaries may use their access to our supply chain to pursue and gain access to sensitive Lockheed Martin systems and technologies. These entities also may intentionally substitute counterfeit parts or compromised systems into products destined for Lockheed Martin technologies and as a result degrade the performance of these technologies.

WHAT CAN YOU DO?

You can work with other Business Area partners to develop and employ a corporate-defined list of requirements to address supply chain risks, threats and vulnerabilities. These requirements should be monitored and reevaluated in order to stay relevant to the changing environment.

- Develop a supply chain risk management policy/plan and define roles and responsibilities for implementing supply chain risk mitigation activities.

- Ensure information distributed externally is limited to what is necessary and sufficient to design, develop, test, produce, deliver and support our programs.

- Identify and document the “criticality” of products and services obtained through our supply chain; this will help us identify, prioritize and mitigate potential supply chain risks.

WHAT CAN YOU DO?
(Continued)

- Supply chain risk is measured by the severity of damage a compromised item would cause. Consider an assessment of the importance of the item and the impact of compromise on operations and assets, individuals, other organizations and the Nation.

- Evaluate suppliers of our suppliers as well as maintenance contracts, which include people and technology, storage facilities and locations, software upgrades after delivery, and packing locations.

- If possible, diversify/disperse how the product is acquired in order to make it difficult for an adversary to determine how, when and where an element will be acquired.

- Consider potential supply chain risks throughout the life cycle and don't just accept system products/elements "as they are"; manage any risks after delivery.

- If you believe you've observed suspicious incidents regarding the supply chain, or if you'd like to learn more about your role in guarding against intelligence threats to our Corporation, contact your Business Area security team for assistance.