Supplier Training Excellence Program

Cybersecurity Webinar

February 9, 2017
Agenda

• Why must my company complete the Cyber Questionnaire(s)?
• What are the Cyber Questionnaire(s)?
• How do I get help? What do I focus on first?
Why am I being asked to complete a Cyber Questionnaire?
Problem

I want to mention the serious problem of the loss of unclassified sensitive information to industrial espionage. Some have called the loss of this information through our networks the greatest transfer of wealth in history….providing potential adversaries with huge savings in time and money as they seek to develop weapon systems comparable, and even superior, to our own.

Mr. Frank Kendall, former Undersecretary of Defense for Acquisition, Technology and Logistics
(2013 LM Supply Chain Conference)
The Director of National Intelligence has identified Supply Chain cyber risk as a threat to the National Security of the United States and released this video highlighting Supply Chain Cyber Risk.

Office of the Director of National Intelligence’s National Counterintelligence Video: Supply Chain Risk Management

https://www.youtube.com/watch?v=oj5iD0D7JsY&feature=youtu.be

Office of the Director of National Intelligence’s National Counterintelligence release of Supply Chain Risk Management Video:


Your Cyber Vigilance is Critical to our National Security
Understanding the Cyber Threat Scope

- Spear Phishing
- Nation State
- Core Network
- Espionage

2005

- Mobile
- Social Media
- Watering Hole
- Web Server
- Spear Phishing

2016

- Supplier
- Joint Venture
- Mobility
- Core Network
- Cloud
- Platform
- Perimeter
- Espionage (IP Theft)
- Espionage (Intel)
- Disruptive (DDoS)
- Financial
- Destructive

© 2017 Lockheed Martin. All Rights Reserved.
What am I required to do for Lockheed Martin?
Supply Chain Cyber Initiative Strategy

Collaboration
- Supply Chain
- Cybersecurity
- Program Management
- Engineering

End Goal
- Known Supplier Cybersecurity Posture
- Supplier Cybersecurity Validation
- Supplier Threat Awareness
- Supplier Cybersecurity Capability Improvements

Move Defenses “Up Stream”
Industry Collaboration & Supplier Engagement

Understand Supplier Posture

**Cybersecurity Questionnaire**
- 180 questions
- APT and risk focus
- Developed by Exostar partners
- Based on standards: Center for Internet Security top Critical Security Controls

**NIST 800-171 Questionnaire**
- 110 questions
- Compliance for Covered Defense Info (CDI) as defined in DFARS 252.204 - 7012
- Requires full compliance by 12/31/2017

- LM chairs the Supply Chain Cybersecurity Working Group
- Exostar hosts cybersecurity questionnaires
- Common supplier expectations
- Supplier inputs once, results shared across multiple primes

© 2017 Lockheed Martin. All Rights Reserved.
Lockheed Martin’s Expectations of our Suppliers

• Suppliers self assess their cybersecurity maturity using Exostar questionnaire(s)
  – Handling Sensitive Information
    • Complete the Cybersecurity Questionnaire
    • Result: Report with Rating/Scores and links to recommendations
    • Define a remediation plan and work to close on open items
  – Handling Covered Defense Information (CDI) as defined by DFARS
    • Be aware of applicable DFARS clauses
    • Flow DFARS requirements to sub-tier suppliers
    • Complete the NIST 800-171 Questionnaire (110 questions)
    • Be compliant with all 110 NIST controls by December 31, 2017
    • Notify DoD CIO of NIST 800-171 non-compliance
    • In parallel notify LM of NIST 800-171 non-compliance
    • Report cyber incidents within 72 hours to DoD CIO
    • Report in parallel cyber incidents within 72 hours to LM
Exostar Cybersecurity Questionnaire

This form contains proprietary and/or confidential information.

In relation to Limitation and Control of Network Ports, Protocols & Services, which of the following Capability Level 4 controls has your organization implemented? Please check all that apply. (ref: EX047)

- Place application firewalls in front of any critical servers
- Verify and validate the traffic going to the server
- Any unauthorized services or traffic should be blocked and an alert generated (CSC 15-7)

Please provide any additional information on your implementation of the Limitation and Control of Network Ports, Protocols & Services controls in the textbox below. This additional information may not be reviewed by all Subscribing Organizations with access to your questionnaire, and it will not have any impact on scoring or capability level. (ref: EX048)

In relation to Mobile Device, which of the following Capability Level 2 controls has your organization implemented? Please check all that apply. (ref: EX087)

- Do all mobile devices (e.g., smartphones, tablets), to include Bring Your Own Device (BYOD) have access control to the device? (CSC 22-1)
- Do all mobile devices (e.g., smartphones, tablets), to include Bring Your Own Device (BYOD) have configuration management to enforce policies provided by a centrally managed infrastructure? (CSC 22-2)
- Do all mobile devices (e.g., smartphones, tablets), to include Bring Your Own Device (BYOD) at a minimum have the ability to remotely wipe the device? (CSC 22-3)

Please provide any additional information on your implementation of the Mobile Device controls in the textbox below. This additional information may not be reviewed by all Subscribing Organizations with access to your questionnaire, and it will not have any impact on scoring or capability level. (ref: EX088)

Guidance

(ref: EX087) The following are Capability Level 2 controls:
- CSC 22-1
- CSC 22-2
- CSC 22-3

There are no Capability Levels 1, 3, 4 & 5 controls for this control family.

Tools for Automating Critical Security Controls:

System/Technical Issues Questions:
PIM Website: www.myexostar.com/pim
Cyber Security/Cyber Security Questions:
Cybersecurity Questionnaire website: www.myexostar.com/pim/Q

Critical Controls FAQ - provides further information on the controls and tools to help implement them.
Process FAQ - Cyber Security Questionnaire provides context of
Which of the following NIST 800-171 controls are fully implemented in your organization? Please check all controls that have been fully implemented by your company. If you would like to add comments regarding the controls (i.e. to offer compensating controls that meet a control on this page, or to note which controls do not apply to your company and the reason why they do not apply) please refer to the last page of this questionnaire. (ref.3.5)

- [ ] 3.5.1 Identify information system users, processes acting on behalf of users, or devices.
- [ ] 3.5.2 Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.
- [ ] 3.5.3 Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.
- [ ] 3.5.4 Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.
- [ ] 3.5.5 Prevent reuse of identifiers for a defined period.
- [ ] 3.5.6 Disable identifiers after a defined period of inactivity.
- [ ] 3.5.7 Enforce a minimum password complexity and change of characters when new passwords are created.
- [ ] 3.5.8 Prohibit password reuse for a specified number of generations.
- [ ] 3.5.9 Allow temporary password use for system logons with an immediate change to a permanent password.
- [ ] 3.5.10 Store and transmit only encrypted representation of passwords.
- [ ] 3.5.11 Obscure feedback of authentication information.

Guidance

For additional information on the DFAR requirements for NIST SP 800-171 please refer to the following:

1. The supply chain representative for the company with which you are working.

2. The NIST special publication NIST SP 800-171 Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

Where do I start?
How do I get help?
Items to Consider

• Does remote access into my environment use Two-Factor Authentication?

• Can employees access my internal company email system from the Internet with a User ID and password?

• Does your company utilize email filtering to identify malicious links, attachments, etc.?

• Does your company use an Internet Proxy Capability to block web browsing to "uncategorized" Web sites?

• Does access to Internet-facing devices/Web servers containing "unclassified sensitive data" require Two-Factor Authentication?
Resources

- Review Lockheed Martin Suppliers Cyber Web page

- Review Supplier Cyber FAQ

- For existing Lockheed Martin Suppliers
  - Complete the Cybersecurity questionnaire in your Exostar profile
Summary

• Aerospace and Defense contractors are targeted
  – You are a target

• Lockheed Martin is working with suppliers
  – To understand their cybersecurity posture
  – To bring a heightened sense of cybersecurity awareness

• Suppliers are responsible
  – To complete the Cybersecurity questionnaire
  – To complete the DFARS/NIST 800-171 questionnaire if applicable
  – To improve their cybersecurity posture as necessary
  – To be compliant with NIST 800-171 by December 31, 2017 as necessary