Supply Chain and Counterintelligence Due Diligence Short

Student Guide

November 2024

Center for Development of Security Excellence

Contents

Supply Chain and Counterintelligence Due Diligence Short

Introduction

Adversaries seek to cause harm to the United States through exploitation of our trusted insiders, attacks on our cyber networks and systems, espionage, and even terrorism. Foreign intelligence entities, or FIEs, will use any means available to harm our national security. It is critical for you as a trusted insider to be diligent in reporting all suspicious activity.

In this Short, you will learn the risks posed to our supply chain by FIEs and how you can support supply chain counterintelligence, or CI due diligence to mitigate these risks.

Here is the objective:

- Given a scenario, determine whether there is a supply chain risk and the appropriate action to take if there is.

Definitions

When discussing the supply chain, we refer to the companies, materials, and systems involved in manufacturing and delivering goods. It is the chain of processes and businesses involved in producing and distributing a commodity. Due diligence refers to the proactive process or set of steps that a reasonable person should take to prevent harm to persons or property. For example, researching a potential vendor before completing a transaction with them.

Apply a due diligence process from a CI perspective to protect your supply chain from FIEs and other adversaries.

Supply Chain Risk Management

Supply Chain Risk Management, or SCRM, is a multistep process that provides a framework for collecting and evaluating information to:

- Identify assets
- Assess threats and vulnerabilities
- Determine the impact of loss, damage, or compromise of assets
- Develop and apply countermeasures
- Monitor and re-evaluate

Supply chain risks exist across all phases of the life cycle.

Methods

Take a moment to review these methods of supply chain disruption and exploitation.

- Cyber intrusions on corporate systems and/or unwitting suppliers
- Co-opted suppliers, especially sub-tier/subcontracted suppliers and vendors
- Threats from trusted insiders
- Partnerships with criminal enterprises or adoption of their methods
- Governmental control over foreign suppliers
- Development of front companies, inside and outside the continental United States
- Internal business practices

Signs

Take a moment to review these signs of supply chain compromise.

- Devices exhibiting functionality that was outside the original design
- A device or multiple devices from a lot exhibiting a unique error or failure
- Employees violating security protocols by improperly handling components or introducing non-compliant components
- Dealers offering rare or out of production components at low prices
- Dealers offering short lead times for large orders of components
- Shipping containers showing signs of tampering
- Unclear, vague, or suspicious subcontract vendors or suppliers

What Are Our Adversaries Doing?

FIEs operate online to recruit insiders, witting or unwitting, to gain access to authorized placement and government personnel, facilities, equipment, networks, or systems that someone like you may have. They:

- **Develop legitimate business relationships** with targets, as trusted suppliers or vendors within select supply chains.
- **Exploit the access** and information they acquire.
- **Seek to further expand their access** within target organizations and supply chains.

So, how do adversaries use online activities to exploit human targets?

- Through direct **personal contact** they get information or influence by interacting with people directly, such as manipulation or bribery.
- Through **academic or professional resumes**, they use fake or exaggerated qualifications to access sensitive information or secure important positions.
- Through **phishing** operations, such as fraudulent emails or websites, they trick individuals into revealing sensitive information by pretending to be a trusted entity.
- Conduct **cyber operations** like hacking into systems, installing harmful software, or stealing data, often leveraging previous human exploitation.

So, **who is being targeted**? Any contractors, cleared or uncleared, involved in supplying or installing complete systems or components for DOD or systems, equipment, facilities, procurement programs for other government agencies.

Protecting the Supply Chain

We should strive to identify potential threats to supply chains at early acquisition phases. Implementing certain best practices can help achieve this.

- Identify critical systems, networks, and information by keeping track of all assets and their statuses.
- Focus on protecting the most important systems and data first and use tools and strategies to reduce risks and vulnerabilities.
- Manage third party risk by conducting thorough CI due diligence on: existing and potential vendors or suppliers; mergers and acquisitions; joint ventures; and other types of business relationships. Make sure to include supply chain risks and management terms in contracts.
- Monitor compliance by regularly checking to ensure all parties are following the requirements.

If you see anything that is suspicious, report it using the reporting requirements for DOD personnel that are contained in DOD Directive, or DODD, 5240.02, Change 1, “Counterintelligence.” The requirements for contractors are contained in Title 32 of the Code of Federal Regulations, or CFR, Part 117, the National Industrial Security Program Operating Manual, or NISPOM, rule. Whether you are contractor or DOD personnel, **it is a legal requirement for you to report any suspicious activity or contacts**.

Examples of Reportable Activity

Take a moment to review these examples of reportable activity.

- Devices exhibiting functionality that was outside the original design
- A device or multiple devices from a lot exhibiting a unique error or failure
- Inadvertent or deliberate attempts to break a trusted chain of custody
- Introduction of counterfeit components into a U.S. government system during production
- Unauthorized personnel of any nationality accessing restricted areas of a cleared or uncleared facility involved in the production of components for DOD systems
- Efforts by any individual, regardless of nationality, to compromise an employee involved in manufacturing, assembling, or maintaining DOD systems

Review Activity 1

Imagine you are a product manager at a tech company working for the DOD who has recently discovered some of its devices are exhibiting functionalities not intended in the original design. These functionalities could potentially lead to security vulnerabilities or unexpected user experiences.

If you were in this situation, would you consider this a reportable activity?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

○ Yes, this would be considered a reportable activity and should be reported immediately.

○ No, it’s just a malfunction of the product. An internal review would be sufficient.

Review Activity 2

At a cleared facility that manufactures electronic components for DOD systems, an employee discovers that several individuals who do not have proper identification badges have been seen in restricted areas of the plant. They were observed accessing sensitive production lines where classified components are assembled.

If you were in this situation, would you consider this a reportable activity?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

○ Yes, this would be considered a reportable activity and should be reported immediately.

○ No, there must be a reason those individuals are allowed in the facility.

Review Activity 3

During a routine quality check at a defense contractor's facility, a production line supervisor discovers that several electronic components being assembled do not meet the expected performance specifications. These components, although not counterfeit, are not performing as reliably as certified parts would. The supervisor initiates an internal review to address the issue before proceeding with the assembly.

If you were in this situation, would you consider this a reportable activity?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

○ Yes, this would be considered a reportable activity and should be reported immediately.

○ No, the issue is related to performance, not counterfeiting.

Conclusion

Congratulations. You have completed the *Supply Chain and Counterintelligence Due Diligence Short*. In this Short, you learned about protecting the supply chain from foreign intelligence entities and other adversaries by applying counterintelligence due diligence throughout the supply chain process. You should now be able to determine whether there is a supply chain risk and the appropriate action to take if there is.

Appendix A: Answer Key

Review Activity 1

Imagine you are a product manager at a tech company working for the DOD who has recently discovered some of its devices are exhibiting functionalities not intended in the original design. These functionalities could potentially lead to security vulnerabilities or unexpected user experiences.

If you were in this situation, would you consider this a reportable activity?

◉ Yes, this would be considered a reportable activity and should be reported immediately.

○ No, it's just a malfunction of the product. An internal review would be sufficient.

Feedback*: A device exhibiting unintended functionality would be considered a reportable activity and should be reported immediately.*

Review Activity 2

At a cleared facility that manufactures electronic components for DOD systems, an employee discovers that several individuals who do not have proper identification badges have been seen in restricted areas of the plant. They were observed accessing sensitive production lines where classified components are assembled.

If you were in this situation, would you consider this a reportable activity?

◉ Yes, this would be considered a reportable activity and should be reported immediately.

○ No, there must be a reason those individuals are allowed in the facility.

Feedback*: Unidentified personnel in a secure area would be considered a reportable activity and should be reported immediately.*

Review Activity 3

During a routine quality check at a defense contractor's facility, a production line supervisor discovers that several electronic components being assembled do not meet the expected performance specifications. These components, although not counterfeit, are not performing as reliably as certified parts would. The supervisor initiates an internal review to address the issue before proceeding with the assembly.

If you were in this situation, would you consider this a reportable activity?

○ Yes, this would be considered a reportable activity and should be reported immediately.

⦿ No, the issue is related to performance, not counterfeiting.

***Feedback**: The issue is related to performance rather than counterfeiting, and it's handled internally with corrective measures.*