Supply Chain Threat Awareness

Student Guide

August 2022

Center for Development of Security Excellence

Table of Contents

Course Introduction

Course Introduction

Introduction

Our Nation is dependent upon technologies and capabilities developed and manufactured by our defense industrial base. The defense industrial base is under attack. Our adversaries are stealing and compromising vast amounts of critical technology that jeopardize our safety and security. Ensuring a more capable, resilient, and innovative defense requires that capabilities developed and produced by the defense industrial base are delivered uncompromised. Effective Supply Chain Risk Management mitigates threats from our adversaries.

In this course, you will gain an understanding of the supply chain purpose and policies, threats, and risk mitigation strategies to protect against those threats.

Key Topics:

- Purpose and Policies
- Supply Chain Threats
- Supply Chain Risk Mitigation Strategies

Lessons and Objectives

This course is divided into three lessons: Supply Chain Purpose and Policies, Supply Chain Threats, and Supply Chain Risk Mitigation Strategies.

Before you begin, review the course learning objectives.

Course Learning Objectives:

- Describe the purpose of protecting the supply chain and governing policies
- Identify potential threats to the supply chain
- List risk mitigation strategies used in Supply Chain Risk Management

Lesson 1: Supply Chain Purpose and Policies

Lesson Introduction

Lesson Introduction

In this lesson, you will learn defining aspects of a supply chain and the associated policies and guidelines.

Learning objective.

- Describe the purpose of protecting the supply chain and governing policies

Defining Supply Chain

A simplistic way of defining supply chain is as a system of organizations, people, activities, information, and resources involved in moving a product or service from supplier to customer.

Department of Defense Instruction 4140.01, DOD Supply Chain Materiel Management Policy, uses a more precise definition:

“The linked activities associated with providing materiel to end users for consumption. Those activities include supply activities (such as organic and commercial Inventory Control Points, or ICPs, and retail supply activities), maintenance activities (such as organic and commercial depot level maintenance facilities and intermediate repair activities), and distribution activities (such as distribution depots and other storage locations, container consolidation points, ports of embarkation and debarkation, and ground, air, and ocean transporters).”

Supply chain activities involve the transformation of natural resources, raw materials, and components into a finished product that is delivered to the end customer.

Inventory Control Points (ICPs): The organizational element within a distribution system that is assigned responsibility for system-wide direction and control of materiel including such management functions as the computation of requirements, the initiation of procurement or disposal actions, the development of world-wide quantitative and monetary inventory data, and the positioning and repositioning of materiel

Supply Chain Risk Management (SCRM)

Once we understand supply chain, we can define supply chain risk management, or SCRM. This is the process for managing risk by identifying, assessing, and mitigating threats, vulnerabilities, and disruptions to the DOD supply chain from beginning to end to ensure mission effectiveness.

Successful SCRM maintains the integrity of products, services, people, and technologies and ensures the undisrupted flow of product, materiel, information, and finances across the

lifecycle of a weapon or support system. DOD SCRM encompasses all sub-sets of SCRM, such as cybersecurity, software assurance, obsolescence, counterfeit parts, foreign ownership of sub-tier vendors, and other categories of risk affecting the supply chain.

SCRM Purpose

Supply Chain Risk Management helps mitigate conditions that can reduce the impact of the critical manufacturing capacity and availability and integrity of critical goods, products, and services.

The addition of the Prepare Step is one of the key changes to the RMF—incorporated to achieve more effective, efficient, and cost-effective security and privacy risk management processes.

Building resilient supply chains will protect the United States from facing shortages of critical products. It will also facilitate needed investments to maintain America's competitive edge in research and development, strengthen U.S. national security, revitalize and rebuild domestic manufacturing capacity, and create well-paying jobs. Secure supply chains are crucial to maintaining a healthy economy. Given the impact supply chains have on the entire Nation, our adversaries see them as targets to exploit in order to weaken the Nation.

Supply Chain Policies and Executive Orders

Over the past decade, adversaries to the United States, to include foreign intelligence entities, or FIEs, strategic competitors, and criminal actors, have exploited vulnerabilities in the DOD supply chain. This has been accomplished through numerous means, to include stealing U.S. intellectual property, inserting counterfeit products, and tampering with products along the supply chain to name a few. This has the net effect of decreasing confidence in the security of products delivered to the DOD.

Policies have been developed to guide the DOD in securing the supply chain. These policies and Executive Orders include:

- Executive Order, or E.O., 14017,
- DOD Manual, or DODM, 4140.01,
- DOD Instruction, or DODI, 4140.01,
- DODI 4140.67,
- DODI 5000.90,
- DODI 5200.44, and
- DODI O-5240.24

Let's have a brief overview of each.

Supply Chain Policies (cont.)

To strengthen the national industrial base during times of disruption, President Joseph R. Biden, Jr. signed Executive Order, or E.O., 14017, America's Supply Chains, on February 24, 2021. The E.O. calls for a comprehensive review of supply chains in critical sectors, including the defense industrial base, or DIB.

This includes four 100-day reports on identifying risks in the following supply chains: semiconductor manufacturing and advanced packaging; high-capacity batteries; critical minerals and other identified strategic materials, including rare earth elements; and pharmaceuticals and active pharmaceutical ingredients.

Six one-year reports on industrial bases include: Defense; public health and biological preparedness; information and communications technology, or ICT; the energy sector; transportation; and the production of agricultural commodities and food products.

For more information on this E.O. and the reports, see the Course Resources.

DODM 4140.01, Volumes 1-12: DOD Supply Chain Materiel Management Procedures implements policy, assigns responsibilities, and provides procedures for those who work within or with the DOD supply system.

DODI 4140.01, DOD Supply Chain Materiel Management Policy establishes policy and assigns responsibilities for management of materiel across the DOD supply chain.

DODI 4140.67, DOD Counterfeit Prevention Policy establishes policy and assigns responsibilities necessary to prevent the introduction of counterfeit materiel at any level of the DOD supply chain.

DODI 5000.90, Cybersecurity for Acquisition Decision Authorities and Program Managers establishes policy, assigns responsibilities, and prescribes procedures for the management of cybersecurity risk by program decision authorities and program managers in the DOD acquisition processes.

Cybersecurity Supply Chain Risk Management, or C-SCRM, also has guidelines as provided by the National Institute of Standards and Technology, or NIST. The NIST C-SCRM program helps organizations to manage the increasing risk of supply chain compromise related to cybersecurity, whether intentional or unintentional.

See the Course Resources for more information.

DODI 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks, known as TSN, establishes policy and procedures for managing supply chain risk.

It also implemented DOD's TSN strategy. The TSN strategy integrates robust systems engineering, supply chain risk management, security, counterintelligence, intelligence, information assurance cybersecurity, hardware and software assurance, and information systems security engineering disciplines to manage risks to system integrity and trust.

DODI O-5240.24 CI Activities Supporting Research, Development, and Acquisition establishes policy and assigns responsibilities for conducting and reporting Counterintelligence Functional Services, or CIFS, activities.

Knowledge Check 1

Why is it critical to develop resilient supply chains and protect them?

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

- ○ To maintain a healthy economy
- ○ To protect national security
- ○ To maintain America's competitive edge in research and development
- ○ To mitigate the impact of shortages of critical products

Knowledge Check 2

Match each policy to its description. (*Check your answer in the Answer Key at the end of this Student Guide.)*

DODI 4140.01 _____

DODI 4140.67 _____

DODI 5000.90 _____

DODI 5200.44 _____

DODI O – 5240.24

A. Establishes policy and procedures for managing supply chain risk; implements DOD's TSN strategy

B. Establishes policy, assigns responsibilities, and prescribes procedures for the management of cybersecurity risk

C. Establishes policy and assigns responsibilities for conducting and reporting CIFS activities.

D. Establishes policy and assigns responsibilities necessary to prevent the introduction of counterfeit materiel

E. Establishes policy and assigns responsibilities for management of materiel across the DOD supply chain

Lesson Conclusion

You have completed the Supply Chain Purpose and Policies lesson.

Lesson 2: Supply Chain Threats

Lesson Introduction

Lesson Introduction

A supply chain threat is specific and credible information that a component, system, or service might be targeted by adversaries. Successful exploitation of supply chain would allow FIEs, or foreign intelligence entities, strategic competitors, and criminal actors to manipulate components intended for DOD systems or to gain access to sensitive information.

In this lesson, you will learn about various threats that can impact the supply chain. This lesson is not about greater supply chain resiliency, but about adversarial threat. Factors such as cost, schedule, and performance are important to maintain a resilient and healthy supply chain. Events that may impact resiliency but are not necessarily an adversarial threat include (but are not limited to) civil unrest hampering production, natural disasters stopping transport, and ships getting stuck in a canal. For more information on supply chain resiliency, cost, schedule, and performance, see the course Resources.

Learning objective.

- Identify potential threats to the supply chain

Supply Chain Threats

Secure supply chains are essential to protecting critical infrastructure, countering economic exploitation, and defending against cyber and technical operations.

Activities by foreign intelligence entities, FIEs, or other adversarial attempts aimed at compromising and/or sabotaging the supply chain can occur at any point during the lifecycle. Types of supply chain threats may include counterfeiting, reliability failure, malicious insertion, quality escape, and tampering.

For more information about supply chain threats, visit the Course Resources.

Counterfeit

Counterfeit materiel is any item that is an unauthorized copy or substitute that has been identified, marked, or altered by a source other than the item's legally authorized source and has been misrepresented to be an authorized item of the legally authorized source. This includes relabeled, recycled, or cloned items. The threat to the end consumer is that these items may be defective or may not operate within required parameters.
Within the organization-level, there are seven tasks:

Malicious Insertion

Malicious insertion occurs when an adversary inserts malicious code or a defect into the system with the intent of enabling attacks or causing mission failure. This includes logic bombs, trojan kill switches, and backdoors for access and control.

Tampering

Tampering involves the unauthorized altering of intellectual property using reverse engineering, cyber means, or embedded systems security weaknesses.

Quality Escape

Quality Escape is a defect via mistake or negligence during design, production, or postproduction handling. It may introduce a deficiency or vulnerability and/or degrade life cycle performance.

Reliability Failure

Reliability Failure is a mission failure in the field due to factors unique to military and aerospace environment such as particle strikes, device aging, hot spots, and electromagnetic pulse, or EMP.

Emerging Threats

Emerging Threats refers to new threats, counterfeit trends, security attacks, trust issues that combine multiple threats, or other exploitations of the supply chain.

Knowledge Check 3

Match each potential threat to its description. (*Check your answer in the Answer Key at the end of this Student Guide.)*

Counterfeit _____

Malicious Insertion _____

Tampering _____

Quality Escape_____

Reliability Failure _____

Emerging Threats _____

A. Defect via mistake or negligence during design, production, and postproduction handling

B. Unauthorized altering of intellectual property using reverse engineering, cyber means, or embedded systems security weaknesses

C. New threats, counterfeit trends, security attacks, and trust issues that combine two or more threats

D. Mission failure in field due to factors unique to military and aerospace environment

E. Other than genuine and new devices from the legally authorized source, including relabeled, recycled, cloned, defective, or out-of-spec.

F. Insertion of malicious code or a defect into the system with the intent of enabling attacks or causing mission failure

Lesson Conclusion

You have completed the Supply Chain Threats lesson.

Lesson 3: Supply Chain Risk Mitigation Strategies

Lesson Introduction

Lesson Introduction

Supply Chain Risk Management is essential to protect the confidentiality, integrity, and availability of National Security Systems and to mitigate and manage risks.

In this lesson, Supply Chain Risk Mitigation Strategies, you will learn actions you can take to help protect the supply chain.

Learning Objective:

- List the risk mitigation strategies used in the Supply Chain Risk Management

Risk Management Process

The supply chain is always at risk. Our adversaries seek to exploit U.S. supply chains to sabotage products, disrupt operations, and erode the confidence of the supply chain and materiel.

Organizations should protect against supply chain threats by employing a standardized process to address supply chain risk as part of a comprehensive, defense strategy.

Lesson 1 covered the definition for SCRM. There is a balance between looking at it as a business discipline aimed at understanding and mitigating supplier risk and a more security focused approach of managing risk to the integrity, trustworthiness, and authenticity of products and services within the supply chain. However, either approach benefits from the fundamentals of risk management.

Let's look at each step in the risk management process.

Identify Assets: During this step, you should identify products and services critical to your supply chain. People, Information, Equipment, Facilities, Activities, Operations, and Suppliers, or PIEFAOS, is a DCSA acronym for asset identification.

Assess Threats: A threat is an intent coupled with capability and opportunity to achieve an objective. Take time to assess the intent and capability of adversaries to attack or exploit the products and services identified in the previous step.

Assess Vulnerabilities: When assessing vulnerabilities for each product and service, you should not only identify the vulnerabilities but also the magnitude of those vulnerabilities.

Vulnerabilities may include poor cyber hygiene, improper security policies, or lack of adherence to security policies, to name a few.

Determine Impact: Next, determine the impact of the loss, damage, or compromise for each product and service. This can be measured many ways, to include time lost, money, or loss of life.

Assess Risk: Assess the risk to your supply chain by determining the likelihood that a threat will exploit the vulnerabilities you identified in your supply chain.

Develop Risk Mitigation Strategies: Identify security options that can cost-effectively mitigate risks to the products and services within your supply chain.

Apply Risk Mitigation Strategies: Implement the security options identified in the previous step.

Monitor and Reevaluate: Active monitoring of your supply chain, and the risk mitigation strategies you employ, is critical. Circumstances change. This step allows you to respond to changes to continue to reduce vulnerability and ensure continuity.

The key to managing risk is to mitigate the vulnerabilities introduced through the supply chain as well as vulnerabilities that emerge over the lifecycle of the product or service.

For more information on Supply Chain Risk Management, visit the Course Resources.

Risk Mitigation Strategies at the Higher Level

By exploiting vulnerabilities in our Nation's supply chains, adversaries have proven able to compromise the integrity, trustworthiness, and authenticity of products and services.

To elevate the role of supply chain security, critical strategies include enhancing capabilities to detect and respond to supply chain threats, advancing SCRM supply chain integrity and security across the Federal Government, and expanding outreach to communicate supply chain threats, risk management, and best practices.

Enhance Capabilities

To minimize the threats to key supply chains, existing threat detection, response, and mitigation tools should be leveraged across all aspects of the lifecycle. These tools and capabilities should be optimized for specific supply chains.

Look for tools to:

- Provide automatic updates to threat information and risk mitigations and
- Enable rapid detection and automatic response to threats.

Additionally, you should:

- Utilize supply chain mapping and supply chain illumination tools,
- Conduct business due diligence,
- Incorporate language into contracts and Requests for Information, or RFIs, and
- Ensure your partners have good cyber hygiene.

Advance Integrity

To advance supply chain integrity, supply chain security must be elevated to a top priority and be present throughout the acquisition process. A robust SCRM program illuminates potential security risks and provides risk mitigation strategies to fortify the supply chain. Implementing SCRM programs enables an integrated risk-reduction approach to protect supply chains critical to the U.S. Government and private industry. Successful SCRM programs need enterprise-wide commitment involving multiple disciplines, comprehensive information sharing, and adherence to best practices.

Expand Outreach

Sharing supply chain threat information and mitigation measures with partnering agencies and industries is imperative.

To expand outreach on supply chain threats, risk management, and best practices, you must obtain executive level commitment for a SCRM Program. You also need to identify critical systems, networks, and information and manage third-party risk.

Let's look at each of these methods.

Obtain Executive Level Commitment for a SCRM Program

A successful SCRM program requires commitment from senior stakeholders from across the enterprise, including Security, Information Assurance, Insider Threat, Legal, and Acquisitions.

Horizontal and vertical communication is essential to ensure senior stakeholders' investment in the success of a SCRM program. This includes information sharing to inform risk decisions and implement mitigations.

Organization-wide awareness and training further embeds the SCRM practices with senior stakeholders and empowers employees to manage, mitigate, and respond to supply chain risks.

- Build an Integrated Enterprise Team
- Communicate across the organization
- Establish training and awareness programs

Identify Critical Systems, Networks, and Information

Real-time knowledge of the location and operational status of all assets is essential to understanding what systems, networks, and information are critical to the enterprise.

Identifying critical systems, networks, and information enables stakeholders to prioritize resources for protecting these systems and mitigating supply chain risks.

Continuous monitoring of system data and network performance enables rapid implementation of appropriate risk mitigation strategies to minimize the impact of an attempted disruption or attack.

- Exercise asset management
- Prioritize critical systems networks, and information
- Employ mitigation tools

Manage Third Party Risk

Assess first-tier suppliers regularly to increase visibility into third-party suppliers and service providers. Leverage this data to properly vet vendors who are providing key components to critical systems and networks.

Use SCRM-related security requirements as a primary metric – similar to cost, schedule, and performance – for measuring a suppliers' compliance with the contract. These security requirements include personnel security and system services acquisitions and are fully described in NIST SP 800-161.

Monitor suppliers' compliance to SCRM-related security requirements throughout the supply chain lifecycle, even when terminating supplier relationships.

- Conduct due diligence
- Incorporate SCRM requirements into contracts
- Monitor compliance

Reporting

The introduction of counterfeit or malicious products or materials into the supply chain to gain unauthorized access to classified information, to alter data, disrupt operations, or to interrupt communications related to classified contracts or cleared facilities constitutes a "suspicious contact" and is reportable by cleared companies to DCSA as per the National Industrial Security Program Operating Manual, or NISPOM.

Examples of Reportable Activity

- Devices that exhibit functionality 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 access of restricted areas of a cleared facility involved in the production of components for DOD systems
- Efforts by any individual, regardless of nationality, to exploit or compromise a cleared employee involved in manufacturing, assembling, or maintaining DOD systems. This could include exploiting an expert for their knowledge at a conference or tradeshow, requesting academic reviews or speeches, or coercing an employee to violate a security protocol.

Knowledge Check 4

Which of these are Risk Mitigation Strategies that would protect against supply chain threats?

Select all that apply. (Check your answer in the Answer Key at the end of this Student Guide.)

- ○ Enhance capabilities to detect and respond to supply chain threats
- ○ Advance supply chain integrity and security across the Federal Government
- ○ Expand outreach on supply chain threats, risk management, and best practices
- ○ Identifying susceptibilities, vulnerabilities, and threats throughout the supply chain
- ○ Developing mitigation strategies with the objective of reducing vulnerability and ensuring continuity

Knowledge Check 5

Now try this question.

Which of the following are examples of reportable behavior?

Select all that apply. (Check your answer in the Answer Key at the end of this Student Guide.)

- ○ Broken chain of custody from a supplier
- ○ Multiple products from the same lot experiencing premature failure
- ○ Purchased software pinging (trying to connect to) a foreign military's internet protocol (IP) address
- ○ Employee enters a restricted area to have lunch with their friend

Lesson Conclusion

You have completed the SCRM Risk Mitigation Strategies lesson.

Course Summary

Conclusion

Summary

The Supply Chain Threat Awareness course described the purpose of protecting the supply chain and governing policies, identified potential threats to the supply chain, and listed risk mitigation strategies used in Supply Chain Risk Management.

Course Learning Objectives:

- ✓ Described the purpose of protecting the supply chain and governing policies.
- ✓ Identified potential threats to the supply chain.
- ✓ Listed Risk Mitigation Strategies used in Supply Chain Risk Management.

Course Conclusion

Congratulations! You have completed the Supply Chain Threat Awareness course.
For more information on the Supply Chain, potential threats, Supply Chain Risk Management, and risk mitigation strategies, please visit the Course Resources.
To receive credit for this course, you must take the course exam.

.

Appendix A: Answer Key

Knowledge Check 1

Why is it critical to develop resilient supply chains and protect them?

- **To maintain a healthy economy**
- **To protect national security**
- **To maintain America's competitive edge in research and development**
- **To mitigate the impact of shortages of critical products**

Feedback: *We must build resilient supply chains and protect them for all these reasons.*

Knowledge Check 2

Match each policy to its description

DODI 4140.01 ___E____

DODI 4140.67 ___D____

DODI 5000.90 ___B____

DODI 5200.44 ___A____

DODI O – 5240.24 C_____

A. Establishes policy and procedures for managing supply chain risk; implements DOD's TSN strategy

B. Establishes policy, assigns responsibilities, and prescribes procedures for the management of cybersecurity risk

C. Establishes policy and assigns responsibilities for conducting and reporting CIFS activities.

D. Establishes policy and assigns responsibilities necessary to prevent the introduction of counterfeit materiel

E. Establishes policy and assigns responsibilities for management of materiel across the DOD supply chain

Feedback: *DODI 4140.01 establishes policy and assigns responsibilities for management of materiel across the DOD supply chain.*
DODI 4140.67 establishes policy and assigns responsibilities necessary to prevent the introduction of counterfeit materiel.
DODI 5000.90 establishes policy, assigns responsibilities, and prescribes procedures for the management of cybersecurity risk.
DODI 5200.44 establishes policy and procedures for managing supply chain risk; implements DOD's TSN strategy.
DODI O-5240.24 establishes policy and assigns responsibilities for conducting and reporting CIFS activities.

Knowledge Check 3

Match each potential threat to its description.

Counterfeit ___E____

Malicious Insertion ___F____

Tampering ___B____

Quality Escape ___A____

Reliability Failure __D_____

Emerging Threats ___C____

A. Defect via mistake or negligence during design, production, and postproduction handling

B. Unauthorized altering of intellectual property using reverse engineering, cyber means, or embedded systems security weaknesses

C. New threats, counterfeit trends, security attacks, and trust issues that combine two or more threats

D. Mission failure in field due to factors unique to military and aerospace environment

E. Other than genuine and new devices from the legally authorized source, including relabeled, recycled, cloned, defective, or out-of-spec.

F. Insertion of malicious code or a defect into the system with the intent of enabling attacks or causing mission failure

Feedback: *• Counterfeit refers to products other than genuine and new devices from the legally authorized source, including relabeled, recycled, cloned, defective, and out-of-spec.*

• Malicious insertion involves the insertion of malicious code/defect to enable attacks or cause mission failure; this includes logic bombs, Trojan kill switches, and backdoors for access and control.

• Tampering is the unauthorized altering of intellectual property using reverse engineering, cyber means, or embedded systems security weaknesses.

• Quality Escape refers to a defect via mistake or negligence during design, production, and postproduction handling. It may introduce a deficiency, vulnerability, and/or degrade life cycle performance.

• Reliability Failure is a mission failure in field due to factors unique to military and aerospace environment factors.

• Emerging Threats are new threats, counterfeit trends, security attacks, trust issues that combine multiple threats, and other exploitations of the supply chain.

Knowledge Check 4

Which of these are Risk Mitigation Strategies that would protect against supply chain threats?

- **Enhance capabilities to detect and respond to supply chain threats (correct)**
- **Advance supply chain integrity and security across the Federal Government (correct)**
- **Expand outreach on supply chain threats, risk management, and best practices (correct)**
- ○ Identifying susceptibilities, vulnerabilities, and threats throughout the supply chain
- ○ Developing mitigation strategies with the objective of reducing vulnerability and ensuring continuity

Feedback: *Enhancing capabilities to detect and respond to supply chain threats; advancing supply chain integrity and security across the Federal Government; and expanding outreach on supply chain threats, risk management, and best practices help protect against supply chain threats.*

Knowledge Check 5

Which of the following are examples of reportable behavior?

- **Broken chain of custody from a supplier (correct)**
- **Multiple products from the same lot experiencing premature failure (correct)**
- **Purchased software pinging (trying to connect to) a foreign military's internet protocol (IP) address (correct)**
- **Employee enters a restricted area to have lunch with their friend (correct)**

Feedback: *All of these are examples of reportable behavior.*