Center for Development of Security Excellence

CDSE

Learn. Perform. Protect.

Deliver Uncompromised: Supply Chain Risk Management

Our national defense is largely dependent upon technologies and capabilities developed and manufactured by our defense industrial base. Today, the defense industrial base is under attack. Our adversaries are stealing vast amounts of critical technology that jeopardize our mission readiness, the safety and security of our warfighters, and the security of our citizenry. Ensuring a more capable, resilient, and innovative defense requires that capabilities developed and produced by the defense industrial base are delivered to the warfighter uncompromised. Effective Supply Chain Risk Management can mitigate these risks and ensure that DoD technology is Delivered Uncompromised.

What is a Supply Chain?

What are the threats to my supply chain?

How Can Risk Management Protect my Supply Chain?

SUPPLY CHAIN RISK MANAGEMENT SELF -ASSESSMENT

Do you verify company ownership? Confirm U.S. ownership?
If you use distributors, do you investigate them for potential threats?
Have you identified where additional repair parts will be purchased?
Are all sub-contractors and suppliers located onshore?
Does the program office vet suppliers for threat scenarios?
Do you have documents which track part numbers to manufacturers?
Can you provide a list of who you purchased your COTS software from?
Do you have an awareness regarding the likelihood of counterfeits?
Do you safeguard key program information that may be exposed through interactions with subs and suppliers?
Do you perform reviews, inspections, and have safeguards to detect/avoid counterfeit equipment, tampered HW/SW, vulnerable HW/SW and OPSEC leaks?
Do you use the NES baseline when purchasing software?
Do you comply with ITAR rules?
Do you have procedures to re-create obsolescent parts?

ACCESS THE COMPLETE SCRM SELF-ASSESSMENT TOOL FOR BEST PRACTICES AND RESOURCES

Can you answer these questions? Do you know what the answers mean?

Click here to access the Supply Chain Risk Management Self-Assessment Tool

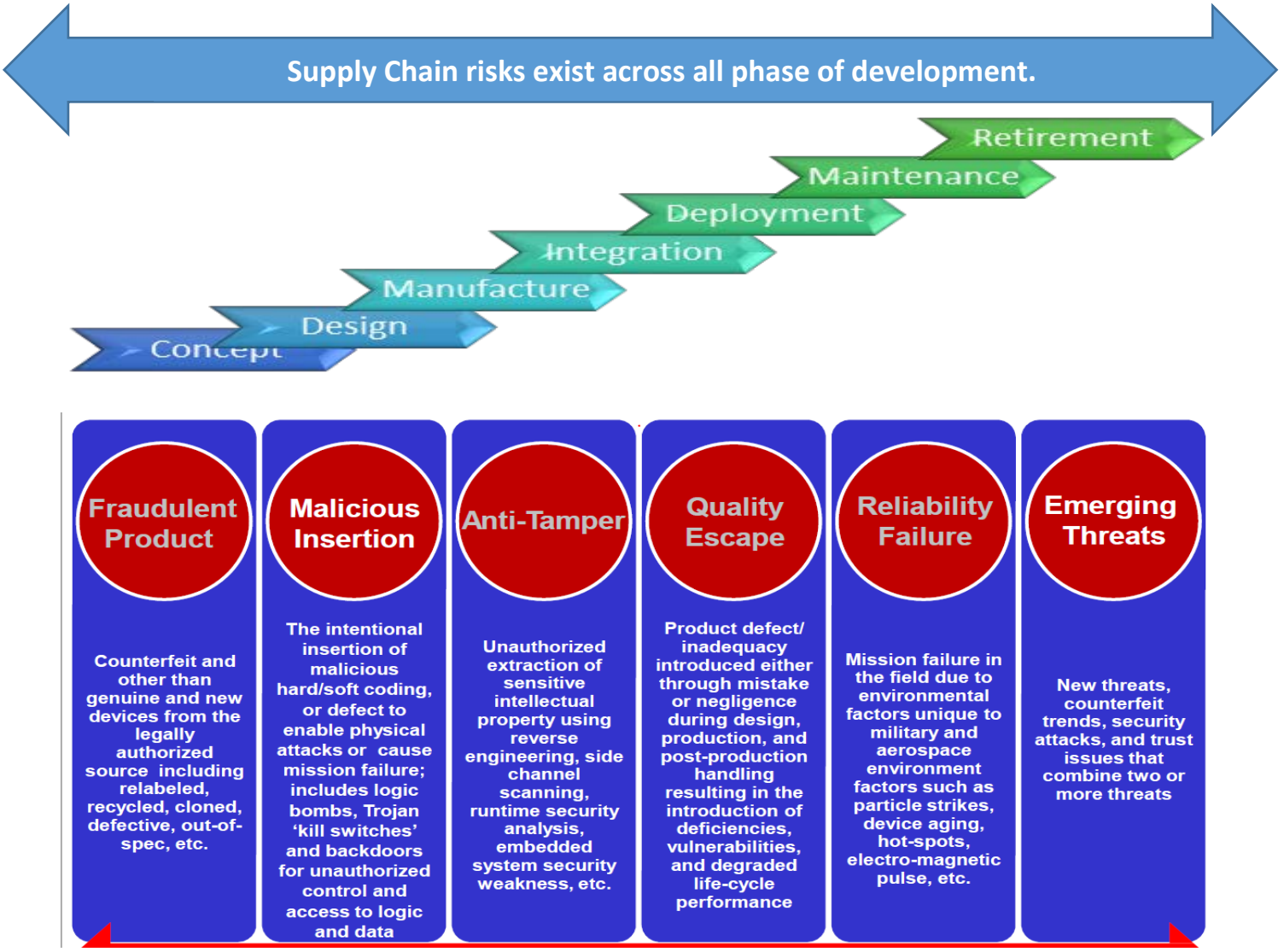
SUPPLY CHAIN

A system of organizations, people, activities, information, and resources involved in moving a product or service from supplier to customer. Supply chain activities involve the transformation of natural resources, raw materials, and components into a finished product that is delivered to the end customer.

SUPPLY CHAIN RISK MANAGEMENT

A systematic process for managing supply chain risk by identifying susceptibilities, vulnerabilities and threats throughout the supply chain and developing mitigation strategies to combat those threats whether presented by the supplier, the supplied product and its subcomponents, or the supply chain.

Click here for more Supply Chain Risk Management Resources.

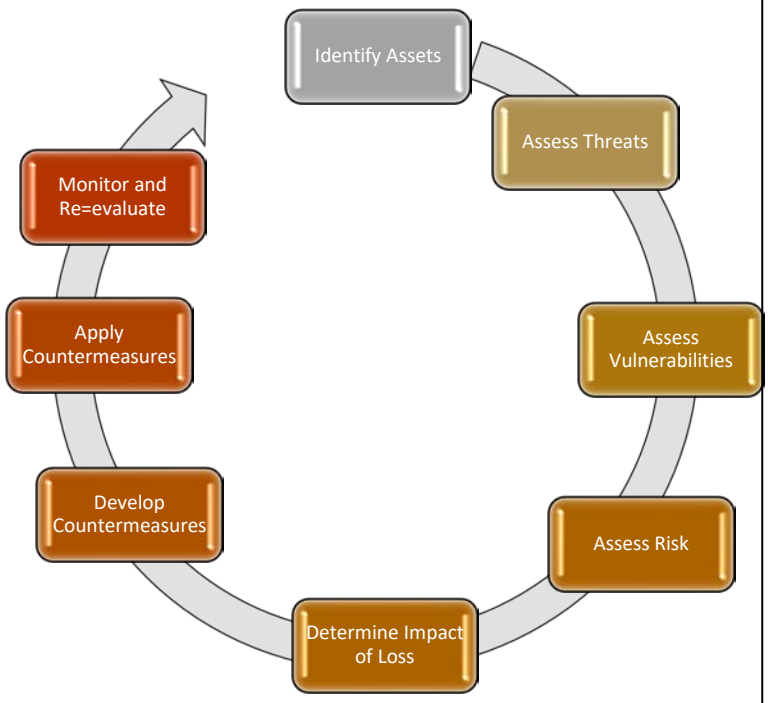


The Risk Management Process

Risk management is a five-step process that provides a framework for collecting and evaluating information to:

- Identify assets (identify value of asset)
- Assess threats (intent and capability of adversaries)
- Assess vulnerabilities (identification and extent of vulnerabilities)
- Determine impact of loss, damage, or compromise of asset
- Assess risks (determine the likelihood that a threat will exploit your vulnerabilities)
- Develop countermeasures (security countermeasure options that can reduce or mitigate risks cost effectively)
- Apply countermeasures
- Monitor and re-evaluate

Click here to learn more about Risk Management



Some Methods of Intelligence Collection Include:

- 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)

Click here to learn more about Collection Methods and Countermeasures.

Potential Countermeasures

- 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
- Encourage supplier site visits by CI personnel for CI Awareness Training
- Conduct Self-assessments
- Consideration of CI Awareness Training requirement in contracts
- Use trusted US manufacturers, builders & installers where possible
- Diversify 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
- Know who’s touching your materials/shipments

Supply Chain Risk Management Self Assessment

Program Name:
Program Manager Name:
Date of Assessment:
Assessor Name:

If answer is "no" to any question, review and apply the "Best Practice" highlighted from the "Key Practices and Implemetation Guide for the DoD Comprehensive National Cybersecurity Initiative 11 Supply Chain Risk Management Pilot Program"

		YES	NO	
	Acquisition			
1	Have you identified your key suppliers?			4.1
2	Do you verify company ownership? Confirm U.S. ownership?			3.2.5
3	If you use distributors, do you investigate them for potential threats?			3.2.5 ®
4	Have you identified where additional repair parts will be purchased?			2.1
5	Are all sub-contractors and suppliers located onshore?			4.8/4.9
6	Does the program office vet suppliers for threat scenarios?			4.6/4.9
7	Do you have documents which track part numbers to manufacturers?			4.9.1
8	Can you provide a list of who you purchased your COTS software from?			4.3.2
9	Do you have an awareness regarding the likelihood of counterfeits			4.5
10	Do you safeguard key program information that may be exposed through interactions with subs and suppliers?			4.2/4.4
11	Do you perform reviews, inspections, and have safeguards to detect/avoid counterfeit equipment, tampered HW/SW, vulnerable HW/SW and OPSEC leaks?			4.6.2
12	Do you use the NES baseline when purchasing software?			4.6
13	Do you comply with ITAR rules?			4.6
14	Do you have procedures to re-create obsolescent parts?			4.7
15	Do you have procedures for securely upgrading software in the field? (Who performs the upgrades?)			4.8
16	Can you prevent from being targeted by malicious actors through the parts acquisition chain?			4.4/4.6
	Design/Development			
17	Are you familiar with all the companies that will work on the design of the product/system?			4.2
18	Does your contractor do all engineering onshore?			3.2.5
19	Do only U.S. citizens have access to your design network?			3.2.5
20	Are you aware of who will develop your training and technical manuals?			4.5
21	If using programmable FPGA chips, do you have a plan to keep them secure?			4.8.7
22	Are you using trusted software development tools?			4.4.4
23	Are you using trusted information assurance controls to safeguard technical data in the development environment (networks, PC's test equipment and configuration systems)?			4.1.3
24	Do you know how to evaluate open source software?			4.4/4.7
25	Are your software compilers controlled for authorized access only?			4.6.4
26	Do you know how your contractor will test and configure software code?			4.6.6
	Logisitics			
27	Does your program have documented configuration management, tracking and version controls in place?			4.3/4.9.4
28	Have you thought about what events (environmental or man-made)can interrupt your supply chain?			4.8.6
29	Are your completed parts controlled, so they are never left unattended or exposed to tampering?			4.2.8
30	Are completed parts locked up?			4.2.6

31	Do you have a process that insures integrity when ordering inventory?			4.2.7
32	Do you periodically inspect your inventory for exposure or tampering?			4.3.3
33	Are upgrades to your IT infrastructure evaluated for possible tampering?			4.3.4
34	Do you have secure material destruction procedures for unused and scrap parts?			4.10.7
35	Is there a documented chain of custody for the deployment of products and systems?			4.3.4
	Policy/Procedures			
36	Do you have definitive policies and procedures that help minimize supply chain risk?			4.3/4.1.3
37	Do you define and manage system criticality and capability?			3.2.5
38	Does everyone associated with the program (program managers, prime contractors, subcontractors, etc.) understand the threats and risks in the program's supply chain?			3.2.6
39	Are all support contractors US citizens?			4.8.2
40	Do you have "insider threat" controls in place?			SC
41	Are you familiar enough with everyone that touches your product or system to know if they pose a threat?			Rev 1
42	Do you use any protective technologies?			4.6.1/4.8.6
43	Do you enter data into the GIDEP database?			GIDEP
43	Do you use, record, and track risk mitigation options throughout the life cycle of the product or system?			4.5/3.2.1
44	Do you have counterintelligence meetings?			Rev 1
45	Have all of your contractors signed non-disclosure agreements?			SF 312
46	Is there foreign national access to your unclassified network?			FOCI
47	Do you make your supply chain risk management policies/procedures a requirement for suppliers?			4.4.1
48	Do your supply chain risk management policies/procedures take into account secondary sourcing?			4.4.1
51	Do you develop and use a Risk Management plan?			RMP
52	Do you have a Risk Management Review Board			sheet two
53	Does anyone have access to your data from an external connection?			4.9.1
54	For contractors who use your data on their system, do they have adequate security controls to protect the data?			4.2

Ten Practices, implemented in their entirety, cover the complete Software Development Lifecycle.	
4.1	**Uniquely Identify Supply Chain Elements, Processes, and Actors**
4.2	**Limit Access and Exposure within the Supply Chain**
4.3	**Establish and Maintain the Provenance of Elements, Processes, Tools, and Data**
4.4	**Share Information within Strict Limits**
4.5	**Perform SCRM Awareness and Training**
4.6	**Use Defensive Design for Systems, Elements, and Processes**
4.7	**Perform Continuous Integrator Review**
4.8	**Strengthen Delivery Mechanisms**
4.9	**Assure Sustainment Activities and Processes**
4.1	**Manage Disposal and Final Disposition Activities throughout the System or Element Life Cycle**