



Supply Chain Security Playbook

Based on NIST SP 800-161 Rev. 1, Update 1, as of Nov. 1, 2024

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited. This material is based upon work supported by the Office of the Secretary of Defense (OSD) Manufacturing Technology (ManTech) Program under Cooperative Agreement HQ00342420005, in the amount of \$5,252,797.59 for the cyber-related activities described herein. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Department of Defense.

Prepared by MxD | Version 1.0 | October 2026

Contents

Why is supply chain security important?.....	3
About this playbook.....	4
The three roles.....	4
How to use this playbook.....	4
Baseline.....	5
Pick your tier.....	5
Plays at a glance.....	6
Play 1: Get leadership backing and establish the team.....	7
Play 2: Build your supplier inventory and rank by criticality.....	8
Play 3: Frame the risk.....	9
Play 4: Write the strategy and policy.....	11
Play 5: Fix how you buy.....	13
Play 6: Assess your suppliers.....	15
Play 7: Choose controls and write the plan.....	18
Play 8: Train your people.....	20
Play 9: Watch, report and repeat.....	21
Appendices.....	23
Appendix A: Scoring grids for Play 6.....	23
Appendix B: The 18 baseline risk factors for Play 6.....	24
Appendix C: Recurring checks.....	25

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

This material is based upon work supported by the Office of the Secretary of Defense (OSD) Manufacturing Technology (ManTech) Program under Cooperative Agreement HQ00342420005, in the amount of \$5,252,797.59 for the cyber-related activities described herein. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Department of Defense.

Why is supply chain security important?

What do you build, and who uses it? If you are part of the defense industrial base (DIB), what you build ends up in a system or device a service member depends on in situations where there cannot be any question about quality and integrity.

The Pentagon has made it clear that supply chain security is a strategic priority. Its first “National Defense Industrial Strategy,” released in January 2024, named resilient supply chains as the first of four priorities and called for better subtler visibility to find and reduce strategic risk.¹

The threat is real: Malicious actors who break into manufacturers mainly seek to collect information and disrupt operations. Verizon’s 2026 breach report lists espionage as a motive in 15% of manufacturing breaches.² The Department of War’s chief information officer says cybersecurity and operational resilience remain critical to protecting American innovation and supporting warfighter readiness. The arsenal of democracy is made by companies like yours, and every supplier that hardens itself is one fewer opportunity for an adversary to exploit.

Contrary to popular belief, security does pay off. IBM’s 2026 breach study found that a business partner or supply chain compromise added more to breach costs than any of the other 30 factors it measured, about \$227,000 on average. These breaches took 258 days to identify and contain. The bill for not proving your diligence can run higher. In 2025, MORSECORP agreed to pay \$4.6 million to resolve False Claims Act allegations that it failed to meet cybersecurity requirements in Army and Air Force contracts.³ On Sept. 1, 2026, the Justice Department announced a settlement of about \$2 million with Honeywell Aerospace over alleged control failures, and the allegations did not involve a breach.⁴

The rules governing security keep evolving in response to the threat, so build principle-based habits. This playbook will help you develop those habits so that you can reduce risk and help ensure what you make will work when it really matters.

¹ <https://defensescoop.com/2024/01/11/ndis-tech-cyber-prioritized-dod-industrial-base-strategy/>

² <https://www.verizon.com/business/resources/executivebriefs/2026-dbir-executive-summary.pdf>

³ <https://www.justice.gov/opa/pr/defense-contractor-morsecorp-inc-agrees-pay-46-million-settle-cybersecurity-fraud>

⁴ <https://www.legal500.com/intelligence/united-states/government-public-sector/dojs-2-million-honeywell-settlement-under-the-civil-cyber-fraud-initiative-what-compliance-failures-mean-for-defense-contractors>

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

This material is based upon work supported by the Office of the Secretary of Defense (OSD) Manufacturing Technology (ManTech) Program under Cooperative Agreement HQ00342420005, in the amount of \$5,252,797.59 for the cyber-related activities described herein. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Department of Defense.

About this playbook

This playbook is designed to walk you through the steps necessary to improve the security of your supply chain in a sound and verifiable fashion. It is derived from NIST Special Publication (SP) 800-161 Rev. 1, “Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations.”⁵

The three roles

Meeting the requirements necessary to secure your supply chain is a team sport. In an ideal situation, you would have ample human resources at your disposal. The reality is that you almost certainly do not have individuals dedicated to security or compliance efforts of any kind, much less something as complicated and far-reaching as cybersecurity supply chain risk management (C-SCRM). That’s OK. If one person has to wear more than one hat (or all of them), diligence is what matters. Make clear which hat you are wearing at each point in the process, and document your decisions and actions in that role.

Role	NIST level	Responsibilities
Leader	Level 1, Enterprise	Sets direction. Defines the strategy and policy, sets risk appetite, makes company-wide decisions and funds the work.
Program owner	Level 2, Mission and business process	Applies the direction to a business line. Manages supplier relationships, writes procedures, sets risk tolerances and reports upward.
System owner	Level 3, Operational	Applies it to a single system or purchase. Writes the C-SCRM plan, picks and tailors controls and reports upward.

How to use this playbook

Every play starts with a goal and a reference to a tab in this playbook’s sister publication, “Supply Chain Evidence Workbook.” The numbered steps that follow should be worked by the appropriate member of your team. Plays end with a list of items to retain as evidence of compliance, followed by the approvals or sign-offs required for your work.

We cannot account for the size, nature and structure of every company in the DIB, so this guidance is an attempt to strike a middle ground. Not everything will apply in every circumstance; use your best judgment when deciding what to leave out or modify.

⁵ <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1-upd1.pdf>

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

This material is based upon work supported by the Office of the Secretary of Defense (OSD) Manufacturing Technology (ManTech) Program under Cooperative Agreement HQ00342420005, in the amount of \$5,252,797.59 for the cyber-related activities described herein. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Department of Defense.

Baseline

There are 17 foundational practices in NIST 800-161r1. Walk through your current policies, practices and other documentation and mark each one as *Done*, *Partly* or *Not Started*, depending on its actual status today, before you do any work. Be as objective as you can. Once you know where you stand, start with the earliest play that holds a practice you marked *Not Started* and work forward from there.

No.	Foundational practice	Your status
1	Establish a C-SCRM program management office or team	Done / Partly / Not Started
2	Obtain leadership support for C-SCRM	Done / Partly / Not Started
3	C-SCRM policies across enterprise levels	Done / Partly / Not Started
4	Define the C-SCRM hierarchy	Done / Partly / Not Started
5	C-SCRM governance structure	Done / Partly / Not Started
6	Well-documented, consistent C-SCRM processes	Done / Partly / Not Started
7	Establish a C-SCRM aware culture	Done / Partly / Not Started
8	Quality and reliability program	Done / Partly / Not Started
9	Build C-SCRM into acquisition and procurement policies	Done / Partly / Not Started
10	Determine Federal Information Processing Standard (FIPS) 199 impact levels	Done / Partly / Not Started
11	Explicit roles for C-SCRM	Done / Partly / Not Started
12	Adequate and dedicated C-SCRM resources	Done / Partly / Not Started
13	Defined C-SCRM control baseline	Done / Partly / Not Started
14	Internal checks and balances to assure compliance	Done / Partly / Not Started
15	Supplier management program	Done / Partly / Not Started
16	C-SCRM included in an established incident management program	Done / Partly / Not Started
17	Processes to ensure suppliers disclose vulnerabilities	Done / Partly / Not Started

Pick your tier

NIST 800-161r1 uses the four NIST Cybersecurity Framework (CSF) Tiers to gauge the maturity of your C-SCRM. Pick the one that fits you today, write it down and date it.

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

This material is based upon work supported by the Office of the Secretary of Defense (OSD) Manufacturing Technology (ManTech) Program under Cooperative Agreement HQ00342420005, in the amount of \$5,252,797.59 for the cyber-related activities described herein. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Department of Defense.

Tier	Description
1	You do not understand your exposure to supply chain risk or your role in the larger ecosystem. You have no processes to find, assess and reduce that risk.
2	You understand your supply chain risk and your role. You have not yet formalized how you manage that risk or how you share information with others.
3	Policies, processes and procedures for managing supply chain risk are in place, followed and monitored. People have the skills for their roles. You have formal agreements that pass baseline requirements to suppliers and partners.
4	You take in and share information with partners, and you use real-time or near-real-time information to improve security before an event happens.

You should reevaluate your tier regularly. Choose the interval that suits you, and once you decide, block off that time on the calendar so you don't forget to do it.

Plays at a glance

Play	Title	Role	What you finish with
1	Get leadership backing and establish the team	Leader	Named lead, charter, budget list
2	Build your supplier inventory and rank by criticality	Program owner	Dated inventory and critical list
3	Frame the risk	Leader	Signed assumptions, limits, risk appetite and tolerance
4	Write the strategy and policy	Leader	Approved strategy and policy
5	Fix how you buy	Program owner	Buying rules and contract terms
6	Assess your suppliers	Program owner	Assessment record for each priority supplier
7	Choose controls and write the plan	System owner	Approved C-SCRM plan for each priority system
8	Train your people	Leader	Role-based training and records
9	Watch, report and repeat	Program owner	Monitoring strategy, reports and triggers

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

This material is based upon work supported by the Office of the Secretary of Defense (OSD) Manufacturing Technology (ManTech) Program under Cooperative Agreement HQ00342420005, in the amount of \$5,252,797.59 for the cyber-related activities described herein. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Department of Defense.

Play 1: Get leadership backing and establish the team

Roles	Leader (Level 1)
Goal	Name who is in charge, who is on the team and where funding comes from.
Workbook Tab	Decisions and Sign-Offs

1. Name one executive-level person, office or group to lead supply chain risk work for the company. Have the head of the organization confirm in writing that this person can make supply chain risk decisions.
2. Pull together a team from the functions that touch your supply chain: IT, security, procurement, risk management, engineering and legal, as examples. In a small company one person may cover several roles; write down who covers which.
3. Write a charter for the team. Include goals, objectives, authorities, meeting schedule and responsibilities. Decide how often the team will meet.
4. Define responsibilities in writing. Cover at least four jobs: collecting supply chain threat information, running risk assessments, choosing and applying mitigations, and monitoring.
5. Decide whether decisions are made in one place or spread across business lines. The details of “how” are up to you.
6. Build a budget list with two columns, one-time costs and recurring costs. Recurring cost lines include personnel, contracts, training, tools and systems. Look at existing funds and shared services before you ask for new money.
7. Give C-SCRM its own line in the budget, tied to performance measures.

Keep as evidence

- The written designation of the C-SCRM lead
- The signed charter
- Role assignments, with who covers each role
- The budget list, with a funding source for each line
- Notes from a team meeting showing the team has met

Approvals/sign-off

The head of the organization signs the charter and the supply chain lead designation.

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

This material is based upon work supported by the Office of the Secretary of Defense (OSD) Manufacturing Technology (ManTech) Program under Cooperative Agreement HQ00342420005, in the amount of \$5,252,797.59 for the cyber-related activities described herein. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Department of Defense.

Play 2: Build your supplier inventory and rank by criticality

Roles	Program owner (Level 2), with input from System owners (Level 3)
Goal	Know who supplies what, and which suppliers matter most.
Workbook Tab	Supplier Inventory

1. List every supplier, every contract and the products or services each one provides. Include sources outside purchasing, such as open-source software, an in-house shared service or a product reused for a new need.
2. Define criticality for your company. Critical processes are the ones that, if disrupted, corrupted or disabled, are likely to degrade or fail the mission.
3. Sort suppliers into groups: mission-critical, sustaining and standard or nonessential. Use names and criteria that fit your company.
4. For each tier-one (direct) supplier, record four things: the contract or order ID; what the supplier provides; the program, project or system that uses it; and its criticality level. Who qualifies as a “tier-one” supplier is up to you.
5. Work top down. Start with the critical processes, then the systems that support them, then the components those systems depend on. Then work bottom up. For each component, ask what happens to the system and the process if it fails or is compromised.
6. Look for single points of failure among your suppliers and their suppliers. Two suppliers of raw materials are not really two suppliers if they both rely on the same subcontractor.
7. For low-impact systems, check for links to moderate- and high-impact systems. Would failure of a low-impact system have cascading effects?
8. To the extent you can, map where critical components are made or developed, how they are delivered and how information and money flow.
9. Date your list and review your analysis at least once a year.

Keep as evidence

- The supplier inventory
- A one-page statement of how you decide criticality
- The dated critical-supplier list
- The list of single-source items

Approvals/sign-off

The Program owner approves the inventory and the ranking. The Leader receives the critical list.

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

This material is based upon work supported by the Office of the Secretary of Defense (OSD) Manufacturing Technology (ManTech) Program under Cooperative Agreement HQ00342420005, in the amount of \$5,252,797.59 for the cyber-related activities described herein. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Department of Defense.

Play 3: Frame the risk

Roles	Leader (Level 1), then Program owner (Level 2)
Goal	Write down the assumptions, limits, risk appetite and trade-offs that guide every later decision.
Workbook Tab	Decisions and Sign-Offs

Assumptions

1. List your assumptions about threats, vulnerabilities, impacts and likelihoods in your supply chain. Name the processes and systems that make up your supply chain, including contracted services and commercial products.
2. Use the four threat source types specified in NIST 800-161r1: adversarial attacks, accidental human error, structural failures such as equipment failure, and environmental threats such as disasters and geopolitical disruption.
3. Set a repeatable way to rate each system's impact. For each system, rate confidentiality, integrity and availability as low, moderate or high. The highest rating sets the overall level. Write down your methodology.

Constraints

List what limits you: policies, laws and regulations, mission and business processes, resource limits, acquisition rules, and available, mandated or restricted sources of supply.

Risk appetite and tolerance

1. Write a risk appetite statement. Risk appetite is the type and amount of risk you will accept to reach your goals. If you have no risk appetite statement, write one for the C-SCRM program.
2. Write risk tolerance statements. Tolerance is how much risk you will bear after you respond. Tolerance statements put risk appetite to work for Level 2 and Level 3 decisions. You are free to establish your own measures and limits.
3. Pick measures to track against these statements, such as key performance indicators and key risk indicators. Name where each measure's data comes from.

Priorities and trade-offs

Write down which goals take priority when they conflict. For example: favor existing supplier relationships over new ones, favor standard security practices over product-team independence, favor parts made in certain regions to avoid geopolitical risk. Criteria are yours to establish.

Check the outputs

1. Confirm you have all the necessary outputs: a C-SCRM policy, criticality (including prioritized processes and impact levels), assessment method and guidance, response guidance, monitoring

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

This material is based upon work supported by the Office of the Secretary of Defense (OSD) Manufacturing Technology (ManTech) Program under Cooperative Agreement HQ00342420005, in the amount of \$5,252,797.59 for the cyber-related activities described herein. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Department of Defense.

guidance, business requirements, revised processes and architecture, operational-level requirements and acquisition security requirements.

2. Decide when you will reframe risks. You can do it at set intervals that make sense for your organization (annually or twice a year, for example) or when triggers you establish occur, such as business changes or new insight.

Keep as evidence

- A dated record holding your assumptions, constraints, risk appetite and tolerance statements, priorities and trade-offs
- The impact-rating method
- The list of measures and their data sources

Approvals/sign-off

The head of the organization, or the person to whom that authority is delegated, signs the risk appetite and tolerance statements. The Program owner signs the Level 2 version for each business line.

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

This material is based upon work supported by the Office of the Secretary of Defense (OSD) Manufacturing Technology (ManTech) Program under Cooperative Agreement HQ00342420005, in the amount of \$5,252,797.59 for the cyber-related activities described herein. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Department of Defense.

Play 4: Write the strategy and policy

Roles	Leader (Level 1), with the Program owner (Level 2)
Goal	Put your direction into two short documents that people can follow: a C-SCRM strategy and plan, and a C-SCRM policy.
Workbook Tab	Decisions and Sign-Offs

How and where to document

1. Choose how to document your C-SCRM processes: inside your existing documents, in separate C-SCRM documents or a mix. All three are acceptable.

Strategy and plan

1. Build a strategy and plan using the template in NIST 800-161r1.
2. List the laws, regulations, contract clauses and standards that govern your program.
3. Choose your strategic objectives.
4. Build a milestone table with columns for milestone, status, owner, priority and target date.
5. Set how often the strategy is reviewed. Once a year is fine as long as there are no major changes that would affect your objectives.

Policy

1. Build the policy from the template in NIST 800-161r1. Policy may be written at Level 1, Level 2 or both.
2. State the program's purpose, who is responsible, what authority each role holds and how compliance is enforced. Show where C-SCRM connects to your risk management process and your system development life cycle.
3. Set the review period. Once a year should be fine unless there is a reason to revise sooner: a change in related policies, a significant C-SCRM event, a new technology, a newly found vulnerability, an operational or environmental change, a shortcoming in the policy or a change of scope.
4. Keep a version table with version number, date, description of change, sections affected and who made the change.
5. Tell staff, contractors and suppliers when the policy changes.

Keep as evidence

- The signed strategy and plan, with milestone table
- The signed policy, with version table
- A record of who received each version

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

This material is based upon work supported by the Office of the Secretary of Defense (OSD) Manufacturing Technology (ManTech) Program under Cooperative Agreement HQ00342420005, in the amount of \$5,252,797.59 for the cyber-related activities described herein. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Department of Defense.

Approvals/sign-off

The head of the organization, or the person to whom that authority is delegated, approves both documents.

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

This material is based upon work supported by the Office of the Secretary of Defense (OSD) Manufacturing Technology (ManTech) Program under Cooperative Agreement HQ00342420005, in the amount of \$5,252,797.59 for the cyber-related activities described herein. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Department of Defense.

Play 5: Fix how you buy

Roles	Program owner (Level 2), with the Leader approving the rules and System owners (Level 3) applying them
Goal	Build supply chain checks into every step of buying.
Workbook Tab	Decisions and Sign-Offs

Set the rules

1. Add a security requirements checklist to purchase requests. Also cover charge card purchases of IT or operational technology (OT).
2. Keep a prohibited-supplier list where law or regulation calls for one. Keep an approved or preferred supplier list that meets your security requirements.
3. Buy from original manufacturers or their authorized distributors and resellers when you can. Use open-source software only from vetted and approved libraries.
4. Do not use “lowest price technically acceptable” source selection for IT or OT purchases.
5. Write down when secondary market parts are allowed, if ever.

Run each purchase

1. Form a purchase team: someone from the program, someone with technical and security knowledge and someone from procurement.
2. Plan the buy: Write down the need and how critical it is. Criticality tells you how much risk you can tolerate on a purchase.
3. Write supply chain security requirements next to your performance, schedule and cost requirements. Pick controls that fit this product or service.
4. Research who sells the item and how concentrated the market is. Use requests for information or due diligence questionnaires as a screen.
5. Score supply chain criteria when you pick a source. Review each bidder against your requirements and look at its security record.
6. Before you accept delivery, check the quality of the product or its components, look for vulnerabilities and confirm authenticity. Finish this before deployment.
7. For critical items, consider tamper-evident packaging, trusted or controlled distribution, filtered or blind buys or concealing the part’s end use.
8. Ask for a software bill of materials (SBOM) for software and logic-bearing hardware where it applies. SBOMs help with provenance; they do not replace vulnerability management or vendor risk assessments.
9. Write rules for emergency buys, including who can approve an exception and on what grounds. Buying outside your normal process adds risk.

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

This material is based upon work supported by the Office of the Secretary of Defense (OSD) Manufacturing Technology (ManTech) Program under Cooperative Agreement HQ00342420005, in the amount of \$5,252,797.59 for the cyber-related activities described herein. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Department of Defense.

Write the contract

1. Have your legal team draft C-SCRM contract language.
2. Make meeting your security requirements a condition of award.
3. Require suppliers to pass requirements down to their subcontractors where they apply. Tie each supplier's C-SCRM performance goals to objective evaluation criteria. Research fourth- and fifth-party suppliers (suppliers further down the chain) before award.
4. Require periodic revalidation that a supplier still meets your requirements. Set the interval yourself and document it so it gets done.
5. Spell out each party's role and actions when a supply chain risk or incident occurs. Determine how vulnerabilities, incidents and disruptions get reported to you, and define what counts as serious. Require suppliers to find vulnerabilities in their products and disclose them promptly.
6. Include grounds to terminate the contract if risk rises beyond what can be reduced to an acceptable level.
7. Add acquisition process items: remediation of emerging vulnerabilities, intellectual property (IP) ownership, expected product life and end-of-life options, spare parts and alternate sources, acceptance criteria for what you receive and monitoring of supplier systems in the supply chain.
8. Pick how you will verify the supplier: certifications, site visits, third-party assessments or self-attestation. Match the rigor to how critical the item is. Let suppliers reuse existing evidence, such as an ISO 27001 certification.
9. Ask critical suppliers to set up notification agreements with the parties in their own supply chain that play a role in your critical product or service.

Keep as evidence

- The purchase security checklist
- The prohibited-supplier and approved-supplier lists
- Your contract language for C-SCRM terms, reviewed by legal
- A completed checklist for one real recent purchase

Approvals/sign-off

The Leader approves the buying rules. Legal reviews the contract language.

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

This material is based upon work supported by the Office of the Secretary of Defense (OSD) Manufacturing Technology (ManTech) Program under Cooperative Agreement HQ00342420005, in the amount of \$5,252,797.59 for the cyber-related activities described herein. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Department of Defense.

Play 6: Assess your suppliers

Roles	Program owner (Level 2), with System owners (Level 3) supplying system facts
Goal	Rate the risk of each priority supplier and product, and record how you reached the rating.
Workbook Tabs	Supplier Assessment, Assessment Questions, Risk Factors, Screening Log, Scoring Grids

Set priorities

1. Start with critical suppliers and critical systems. Rank the rest so lighter checks go to lower-priority suppliers. Priority should determine how rigorous each assessment is.
2. Use one consistent set of factors for every supplier. That lets you compare suppliers with one another over time. Document where each piece of information came from.

Screen for restricted sources

1. Check each supplier against the items in the restricted-source screening table at the end of this play. Record the date, the result and who checked.
2. If a supplier appears on a restricted or prohibited list, pause the assessment and escalate to your leadership and legal counsel.

Gather the facts

1. Send the scoping questionnaire in NIST 800-161r1 to prospective suppliers. The template is a toolbox; use only the questions that match the controls you expect to apply (see Play 7).
2. Research the baseline risk factors in NIST 800-161r1 Table 28 (listed in Appendix B). For critical suppliers, work through all risk factors. Note “no information found” when that is the case. Findings can be positive, neutral or negative.
3. Read findings together, not one at a time. One risk indicator does not prove a supplier is unacceptable, and it does not tell you how severe the risk is. If you are unsure, do more research or escalate.
4. Record the source of each fact and how confident you are in it. Good information is timely, relevant, unbiased, reasonably complete and credibly sourced.

Rate the risk

1. Rate the threat as Critical, High, Moderate or Low. The rating rests on the threat actor’s capability and intent.
2. Rate the vulnerability as Critical, High, Moderate or Low. The rating rests on how exposed the supplier or product is and how easily it can be exploited.
3. Rate the impact as Critical, High, Moderate or Low. The rating rests on the harm if the product, service or supplier is lost, damaged or compromised.
4. Combine the ratings with the two grids in Appendix A. Threat and vulnerability give you likelihood. Likelihood and impact give you overall risk. If you find several vulnerabilities, rate each one.

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

This material is based upon work supported by the Office of the Secretary of Defense (OSD) Manufacturing Technology (ManTech) Program under Cooperative Agreement HQ00342420005, in the amount of \$5,252,797.59 for the cyber-related activities described herein. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Department of Defense.

Record and decide

1. Write the assessment record. Include who did the assessment and when; a profile of the supplier; a description of the product; the purpose and life cycle phase; the method used and any departures from it; findings and analysis; impact; options to reduce unresolved risk; the risk level and why; the response; and review and clearance.
2. Choose a response: accept, avoid, mitigate, transfer or share. Weigh it against your risk appetite and tolerance, and against the mitigations you could put in place.
3. Have the person who owns the risk sign the decision. Match the signer to how far the impact reaches.
4. Set a schedule for reassessing this supplier and list the events that trigger an earlier look (see “Triggering events” in Play 9).
5. Protect the data you collect about suppliers.

Restricted-source screening table

No.	Item	Screening Criteria
1	Specially Designated Nationals and Blocked Persons List (Treasury)	Parties found responsible for malicious cyber-enabled activity. An entity owned 50 percent or more by blocked persons is itself blocked. U.S. persons may not deal with blocked persons.
2	Sectoral Sanctions Identifications List	Persons operating in listed sectors of the Russian economy. Restrictions cover transactions, financing, and some debt dealings.
3	Foreign Sanctions Evaders List	Foreign persons found to have violated, tried to violate, or helped others violate U.S. sanctions on Syria or Iran. Transactions with them are prohibited.
4	System for Award Management (SAM) exclusions	Debarred companies excluded from federal contracts, certain subcontracts, and federal assistance.
5	CAPTA List	Foreign financial institutions subject to sanctions, prohibitions, or strict conditions before a U.S. company may do business with them.
6	Persons Identified as Blocked (31 CFR 560)	Property and persons on this list must be blocked if they come within the possession or control of a U.S. person.
7	BIS Unverified List	Listed parties cannot receive items subject to the Export Administration Regulations under a license exception.
8	NDAA Section 889	Unless waived, bars the Federal Government, government contractors, and grant and loan recipients from buying or using covered telecommunications equipment or services from Huawei, ZTE, Hytera, Hikvision, Dahua, and their subsidiaries, when used as a substantial or essential part of a system or as critical technology.
9	Any other federal restriction or law	Any other rule that limits buying from a supplier.

Keep as evidence

- A completed assessment record for each priority supplier

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

This material is based upon work supported by the Office of the Secretary of Defense (OSD) Manufacturing Technology (ManTech) Program under Cooperative Agreement HQ00342420005, in the amount of \$5,252,797.59 for the cyber-related activities described herein. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Department of Defense.

- The screening log with dates and results
- The completed questionnaire and the risk factor worksheet
- Your threat, vulnerability, impact, likelihood and risk ratings
- The signed response decision

Approvals/sign-off

The Program owner signs each assessment record. The person who owns the risk signs the response decision.

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

This material is based upon work supported by the Office of the Secretary of Defense (OSD) Manufacturing Technology (ManTech) Program under Cooperative Agreement HQ00342420005, in the amount of \$5,252,797.59 for the cyber-related activities described herein. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Department of Defense.

Play 7: Choose controls and write the plan

Roles	System owner (Level 3), with the Program owner (Level 2) setting common controls
Goal	Pick the controls that answer your risks, tailor them and write them into a C-SCRM plan.
Workbook Tab	Controls and Evidence

Choose the controls

1. List your response options for each risk you found in Play 6: accept, avoid, mitigate, transfer or share. For mitigation, plan to select and tailor controls.
2. Start from the C-SCRM baseline. Table 6 of NIST 800-161r1 marks the baseline controls in its “C-SCRM Baseline” column. Add more as your assessments call for them. The Workbook tab “Controls and Evidence” lists every control in Table 6, with baseline controls first.
3. Tailor the list. Base your choices on your environment, your operations, the threats you face and the information involved. Get the appropriate officials to approve the tailoring and write down the reason for every addition or removal.
4. Sort controls by who owns them. Level 1 sets common controls for everyone. Level 2 sets common controls for a business line. Level 3 inherits those and adds system-specific controls.
5. Name an owner for each control and set a phased plan, by time or by event, for putting it in place.
6. Check for trade-offs. A control can swap one risk for a bigger one if its dependencies are not understood.
7. Use the SR family controls in the Workbook tab “Controls and Evidence” as a checklist for the supply chain controls. Note that the control text for SR-9, SR-10 and SR-11(3) applies to critical components at a minimum.

Write the plan

1. Write one C-SCRM plan per priority system, as a standalone document. Fold it into the system security plan only if your constraints require it.
2. Capture the following: system name and ID; description; information types and categorization; operational status; diagrams, inventory and life cycle; information exchanges and connections; control details; roles; contingencies and emergencies; related laws and policies; revision and maintenance; plan approval; acronyms; attachments; and plan and life cycles.
3. Include the contents NIST 800-161r1 lists: the Frame environment, the responsible role, key contributors, the controls and measures, tailoring decisions and reasons, feedback among levels, monitoring and enforcement, a review frequency, revision triggers such as life cycle milestones, gate reviews or significant contracting activities and the suppliers involved, where agreements allow.
4. Add a component inventory with these fields: description; version; license number, holder and type; property number; hostname; component type; manufacturer; model; serial number; revision, such as firmware version; physical location; and vendor.

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

This material is based upon work supported by the Office of the Secretary of Defense (OSD) Manufacturing Technology (ManTech) Program under Cooperative Agreement HQ00342420005, in the amount of \$5,252,797.59 for the cyber-related activities described herein. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Department of Defense.

5. For each control, describe how it is implemented, attach the evidence, give the reason for tailoring and name any inherited control.
6. Put the controls that apply into supplier agreements.
7. Get the plan signed and dated.

Check that controls work

1. Test the controls. Use NIST SP 800-53 assessment techniques. Methods may include supplier self-assessment, your own review or third-party assessments. Look first at established third-party assessments and ask for more evidence only where they leave gaps.
2. Review each plan at life cycle milestones, gate reviews and significant contracting activities, at a minimum.

Keep as evidence

- The tailored control list, with the reason for each change
- One C-SCRM plan per priority system, signed and dated
- Component inventories
- Test results or assessor reports for each control you chose to check

Approvals/sign-off

The authorizing official named in the plan signs and dates it.

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

This material is based upon work supported by the Office of the Secretary of Defense (OSD) Manufacturing Technology (ManTech) Program under Cooperative Agreement HQ00342420005, in the amount of \$5,252,797.59 for the cyber-related activities described herein. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Department of Defense.

Play 8: Train your people

Roles	Leader (Level 1) sets the baseline. Program owners and System owners tailor it.
Goal	Make sure every person who touches the supply chain knows their part.
Workbook Tab	Training

1. Name one official to manage C-SCRM training policy and procedures.
2. Add C-SCRM content to your existing security awareness training. Cover your employees and your contractors.
3. Set the baseline training requirements at Level 1. Tailor and refine them at Levels 2 and 3.
4. Make sure everyone learns why C-SCRM matters, what their role is and how to report incidents.
5. Require role-based training for the roles that touch or affect the supply chain: System owners, acquisition, supply chain logistics, system engineering, program management, IT, quality and incident response.
6. Conduct practical exercises that simulate supply chain events, insider threats, social engineering, suspicious communications, advanced persistent threats and the cyber threat environment.
7. Keep records of C-SCRM training, especially for key people in acquisition and security.
8. Feed lessons learned from your C-SCRM work back into the training.

Keep as evidence

- The training policy line and the name of the official who manages it
- The list of roles and the training each one needs
- Training materials
- Completion records for each person

Approvals/sign-off

The official named in step 1 signs off on the role list and the training materials.

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

This material is based upon work supported by the Office of the Secretary of Defense (OSD) Manufacturing Technology (ManTech) Program under Cooperative Agreement HQ00342420005, in the amount of \$5,252,797.59 for the cyber-related activities described herein. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Department of Defense.

Play 9: Watch, report and repeat

Roles	Program owner (Level 2) and System owner (Level 3), reporting to the Leader (Level 1)
Goal	Catch changes early, tell the right people and keep your documents current.
Workbook Tab	Measures, Events Log, Recurring Checks, Decisions and Sign-Offs

Set up monitoring

1. Establish a monitoring strategy. State the purpose, the type and frequency of monitoring, the data you will collect, the measures you will compile, the tools you need, how the data will be protected and the report formats.
2. Draw on these data sources: your own vulnerability and incident management work, manual reviews, information shared with suppliers and others, supplier information and contracts.
3. At your discretion, set regular intervals to review suppliers and their products and services. List the off-cycle events that trigger an early review. Categories may include changes in policy, mission, threat environment, architecture, life cycle or requirements.
4. Build C-SCRM into any continuous monitoring program you already have. If you have none, NIST 800-161r1 says C-SCRM can be the reason to start one.

Respond to events

1. Watch for a triggering event (see “Triggering events,” below). When one happens, reassess the risk, decide whether it is an incident and decide whether you need to share information.
2. In addition to the triggering events listed below, treat these as reassessment triggers: a change in available resources, a change in supply chain cybersecurity risk, a natural disaster or a mission collapse.
3. Add C-SCRM to your incident handling. Cover insider threats tied to supplier personnel with access to your systems, set information-sharing duties with critical suppliers and protect the incident information you exchange with them.
4. Share supply chain risk information through formal channels, such as an Information Sharing and Analysis Center. NIST 800-161r1 warns that informal or unmanaged sharing can create legal risk. Set goals, scope and rules before you share.
5. If a supplier’s work grows to include more sensitive data, refresh the risk assessment.

Report and measure

1. Report to leaders in the form they need. Level 1 reports cover how fully C-SCRM has been implemented, how well it works and your overall exposure. Highlight what needs leadership attention. Agree on the report format with the audience.
2. Pick measures for each level. Level 1: adoption of the policy at lower levels, timeliness of that adoption, adherence to risk appetite and tolerance statements, differences in exposure across business lines, regulatory compliance and customer requirements. Level 2: effectiveness of

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

This material is based upon work supported by the Office of the Secretary of Defense (OSD) Manufacturing Technology (ManTech) Program under Cooperative Agreement HQ00342420005, in the amount of \$5,252,797.59 for the cyber-related activities described herein. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Department of Defense.

mitigation, time spent on C-SCRM activities, exposure by business line, quality of requirement adoption and use of the program office. Level 3: how well the controls are designed, how well they operate and their cost relative to the value they deliver.

3. Give every measure a target and confirm that you can get the necessary data. Set up a feedback loop with the people who use the measures.
4. Recheck your CSF Tier using the “Pick your tier” section.

Keep documents current

1. Feed what you learn back into the C-SCRM plan, then into your assessments and your Frame record.
2. Run recurring checks. The Workbook tab “Recurring Checks” tracks the dates.

Triggering events

- Change of ownership, merger or acquisition
- Disruption to the supply chain for any reason
- New information about a critical vulnerability that may affect technology that the supplier or its supply chain uses
- Discovery of a counterfeit or non-conforming product or component
- A change in where manufacturing or software development happens, especially a move from domestic to foreign locations
- An original manufacturer stops making or supporting a product or critical component
- Evidence of functionality or features that were not disclosed
- A notice that calls for a closer look at whether an attack involving refurbished, tampered or counterfeit information and communications technology (ICT) products affected the confidentiality, integrity or availability of federal data and systems
- Presence of products from a prohibited or otherwise unauthorized source
- Evidence of suspicious foreign ownership, control or influence
- Other changes that may worsen the risk profile, such as loss of key personnel or weaker finances

Keep as evidence

- Your monitoring strategy
- Dated reports to leadership
- The events log, with what you did about each event
- Measures with targets and actuals
- Updated plans and assessments, with version tables

Approvals/sign-off

The Program owner signs the monitoring strategy. The Leader acknowledges each report.

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

This material is based upon work supported by the Office of the Secretary of Defense (OSD) Manufacturing Technology (ManTech) Program under Cooperative Agreement HQ00342420005, in the amount of \$5,252,797.59 for the cyber-related activities described herein. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Department of Defense.

Appendices

Appendix A: Scoring grids for Play 6

Likelihood: Threat by vulnerability

Threat (rows) / vulnerability (columns)	Low	Moderate	High	Critical
Critical	Moderately Likely	Highly Likely	Very Likely	Very Likely
High	Moderately Likely	Highly Likely	Highly Likely	Very Likely
Moderate	Unlikely	Moderately Likely	Highly Likely	Highly Likely
Low	Unlikely	Unlikely	Moderately Likely	Moderately Likely

Overall risk: Likelihood by impact

Likelihood (rows) / impact (columns)	Low	Moderate	High	Critical
Very Likely	Moderate	High	Critical	Critical
Highly Likely	Moderate	Moderate	High	Critical
Moderately Likely	Low	Moderate	High	High
Unlikely	Low	Low	Moderate	High

What each rating means

Rating	Threat	Vulnerability	Impact
Critical	Information shows an adversary is actively engaged in subversion, exploitation or sabotage.	Weaknesses are wholly exposed and easy to exploit.	Failure would cause total enterprise failure or unacceptable degradation that takes exceptional time and resources to recover.
High	Information shows a threat is imminent.	Weaknesses are highly exposed and reasonably exploitable.	Failure would cause severe disruption or unacceptable degradation that takes significant time and resources to recover.
Moderate	Average potential to affect or target you. A specific adversary exists but lacks the capability or the intent.	Weaknesses are moderately exposed and hard to exploit.	Failure would cause serious problems that can be managed quickly with no long-term consequences.
Low	Threats are nonexistent or unlikely, or they have below-average potential to affect or target you.	Weaknesses have limited exposure and are unlikely to be exploited.	Failure would cause few adverse effects, which can be managed quickly with no long-term consequences.

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

This material is based upon work supported by the Office of the Secretary of Defense (OSD) Manufacturing Technology (ManTech) Program under Cooperative Agreement HQ00342420005, in the amount of \$5,252,797.59 for the cyber-related activities described herein. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Department of Defense.

Appendix B: The 18 baseline risk factors for Play 6

For critical suppliers, work through every factor. Write “no information found” where that is true. If you are unsure whether counterfeits matter for the item, include that factor.

Factor	What to look for
Purpose	How the product or service will be used, what else the market offers, how urgent the need is and how long you need it.
Criticality	Whether the item or a part of it supports a mission-critical function or could cause serious harm if compromised.
Information and data	What data the item touches, how much and where it flows. Include any controlled or classified information.
Reliance	How much you depend on the item or source, whether it is a single source and what alternatives exist.
User and operational environment	Where and how the item is used or installed and where the work is performed for labor-based services.
External interdependencies	Data, system or mission links to other organizations, such as shared services.
Functionality, features and components	Built-in security features, who controls them, connectivity needs, bill of materials and any data the item sends out.
Company information	Size, structure, leadership, finances, ownership history, investors and contracts with foreign governments.
Quality and past performance	Track record, customer complaints, recalls, quality metrics and evidence of a quality program.
Personnel	How the supplier vets staff, whether it has an insider threat program, turnover and staffing level.
Physical	Physical security of facilities, closeness to critical infrastructure and natural disaster exposure.
Geopolitical	Location-based unrest or corruption, trade route disruption, legal requirements and regional instability.
Foreign ownership, control or influence	Foreign interests with power over management or operations and ties between the supplier and foreign governments.
Compliance and legal	Record of following laws, regulations and contracts, including sanctions and trade controls, plus fines and judgments.
Fraud, corruption, sanctions and alignment with government interests	Past fraud, debarment or exclusion, history of intellectual property theft or unauthorized technology transfer.
Cybersecurity	The supplier's security practices, past intrusions, unmitigated vulnerabilities and signs of malicious activity.
Counterfeit and non-conforming products	History of counterfeits, gray market sourcing and the supplier's anti-counterfeit controls.

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

This material is based upon work supported by the Office of the Secretary of Defense (OSD) Manufacturing Technology (ManTech) Program under Cooperative Agreement HQ00342420005, in the amount of \$5,252,797.59 for the cyber-related activities described herein. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Department of Defense.

Factor	What to look for
Supply chain relationships, visibility and controls	The supplier's own C-SCRM practices, single-source upstream parts, reliance on a single trade route and product provenance.

Appendix C: Recurring checks

NIST 800-161r1 suggests that the following items be reviewed and updated regularly. You are encouraged to do the same for all aspects of your supply chain security program, but the frequency and level of detail are your call.

Item	What NIST 800-161r1 says
Criticality analysis	Review and update at least once a year.
C-SCRM policy	Sample text: review at least once a year, and sooner if triggers occur.
Risk assessment template	Sample text: review at least once a year.
Strategy and plan	Sample text: at least every three to five years within the federal environment. Your company sets its own interval.
Frame record	Redo at set intervals or when triggers occur. Examples: annually or twice a year.
C-SCRM plans (Level 3)	Review at life cycle milestones, gate reviews and significant contracting activities, at a minimum.
Supplier reassessment	Regular intervals as needed and appropriate.
Supplier inventory	Review and update at a frequency you define.
Supplier revalidation	Periodic.
Risk appetite and tolerance	Monitor and change over time. Update when leadership, strategy, market or conditions change.

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

This material is based upon work supported by the Office of the Secretary of Defense (OSD) Manufacturing Technology (ManTech) Program under Cooperative Agreement HQ00342420005, in the amount of \$5,252,797.59 for the cyber-related activities described herein. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Department of Defense.

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

This material is based upon work supported by the Office of the Secretary of Defense (OSD) Manufacturing Technology (ManTech) Program under Cooperative Agreement HQ00342420005, in the amount of \$5,252,797.59 for the cyber-related activities described herein. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Department of Defense.