



NIST Cybersecurity Supply Chain Risk Management Due Diligence Assessment Quick-Start Guide



U.S. Department of Commerce Gina M. Raimondo, Secretary National Institute of Standards and Technology Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology NIST Special Publication NIST SP 1326 ipd (Initial Public Draft) https://doi.org/10.6028/NIST.SP.1326.ipd October 2024 The public comment period for this draft ends December 16, 2024.

Please send your comments to scrm-nist@nist.gov.

TABLE OF CONTENTS

Navigating This Quick-Start Guide

Title Page.....1

Table of Contents.....2

- Purpose
- What is Due Diligence in C-SCRM?
- Basic vs. Enhanced Due Diligence
- Scope of Due Diligence Quick-Start Guide
- More C-SCRM Resources

Due Diligence, Supplier Reviews, and SCRAs......4

- Relationship to SR-6 & RA-3(1)
- Information Sources

First Steps......5

- Before You Start
- Traceable Company Information
- Contracting and Security Clearance Information
- Consistency Across Findings

Supply Chain Tiers......7

- Illuminating with Tools
- Due Diligence Considerations
- Sub-Tier Supplier Diversity
- Questions to Consider

Foreign Ownership, Control, and Influence......8

- Ownership
- Key Leadership
- Foreign Laws, Policies, and Regulations
- Organization-Defined Parameters

Provenance......9

- Supplier Operational Locations
- Product-Specific Locations
- Research Sources
- Subcomponents

Stability......10

- Organizational Stability
- Product Stability
- Regulatory Compliance Lists
- Historical Data vs. Relevant Information

Foundational Cyber Practices: Suppliers......11

- System Compromises
- User Behavior
- Security Posture
- Data Breaches
- Where to Find Information

Foundational Cyber Practices: Products......12

- Publicly Available Product Information
- SBOM Analytics Findings
- Secure Development Practices
- Supplier Software Attestation

Putting It Together.....13

Due Diligence Findings and Classification......14

- Classifying Due Diligence Findings
- Additional Resources

Learning Recap.....15

- What We Learned
- What's Next
- New to C-SCRM Resources

NIST Due Diligence Assessment Introduction

Purpose

This guide provides cybersecurity supply chain risk management (C-SCRM) program management capabilities with considerations for creating due diligence supply chain risk assessments in accordance with NIST Special Publication (SP) 800-161 (Revision 1). It is a supplement to the content within SP 800-161r1 and is not intended to replace it.

What is Due Diligence in C-SCRM?

From a C-SCRM perspective, due diligence is the investigative process of researching and verifying available information about a given supplier or product prior to entering into an agreement so that informed decisions can be made with all available and pertinent information. Due diligence research is the minimum amount of understanding that an acquirer should have on a supplier and should be done with most of the acquiring organization's suppliers, regardless of criticality.

Basic vs. Enhanced Due Diligence

Basic due diligence is desktop-based research using open sources and publicly available information (PAI) to derive findings. The use of commercial datasets, proprietary sources, and supply chain illumination tools constitutes enhanced due diligence. While some findings categories can be wholly sourced using PAI, others may yield additional results using enhanced toolsets.

Scope of Due Diligence Assessment Quick Start Guide

Due diligence supplier assessments can be applied to any type of supplier, but this Quick-Start Guide is scoped to information and communications technology (ICT) suppliers.



EXPLORE MORE NIST C-SCRM RESOURCES

NIST C-SCRM Project

 ✓ NIST SP 800-161r1
 ✓ C-SCRM Fact Sheet
 ✓ Federal C-SCRM Forum
 ✓ Software and Supply Chain Assurance Forum

Cybersecurity Framework 2.0 C-SCRM Quick-Start Guide

Due Diligence, Supplier Reviews, and SCRAs Relationship to SR-6 and RA-3(1)

Due Diligence and Supply Chain Risk Assessments (SCRA)

Per SP 800-161r1, the C-SCRM Program Management Office (PMO) is responsible for conducting assessments of cybersecurity risks that arise from suppliers seeking to integrate with a given system in accordance with enterprise-wide C-SCRM Level 2 policy requirements. SP 800-161r1 shows that **Cybersecurity Risk** is the **Likelihood** of **Threats** exploiting

Vulnerabilities and causing an Impact to a program or system.

Due Diligence Assessments are a precursor to the SR-6 Supplier Reviews and, in many cases, can serve as the foundation of the Threat and Vulnerability aspects of the RA-3(1) Supply Chain Risk Assessment.

They can be researched and written using PAI, as well as augmented with commercially derived datasets and illumination tools. The components of a Due Diligence Assessment are **Supply Chain Tiers; Foreign Ownership, Control, or Influence (FOCI); Provenance; Stability; and Foundational Cyber Practices.**

5	Supply Chain Risk Assessment (RA-3(1)) (800-53r5/800-161r1) Supplier Review (SR-6) (800-53r5/800-161r1)	 High-level assessment of multiple suppliers within a program or system Threat, Vulnerability, Likelihood, and Impact Criticality analysis and internal infrastructure inputs Comprehensive review specific to one supplier and its products Desktop research as well as supplier questionnaire inputs Threat and Vulnerability considerations 	 Organization-gathered (freely available) Commercial inputs SR-6 Supplier Review Due Diligence Assessments and Sources Supplier inputs RA-3(1) SCRA
on Y	Due Diligence (GV:SC-06) (CSF 2.0)	 Minimum investigative rigor derived from PAI desktop research against one supplier or product Some Threat and Vulnerability considerations 	 SR-6 Supplier Reviews Program/system criticality analysis Supplier criticality analysis
			 Internal infrastructure inputs

INFORMATION

SOURCES

Due Diligence

FIRST STEPS

Pre-Checks and Traceable Company Information



Research Considerations

Pre-Checks: Before You Start

Consider checking the following sources for a snapshot of U.S. Government (USG) regulatory concerns, prohibitions, and exclusions against your research entity to potentially alleviate the need for further research.

- International Trade Administration (ITA)'s <u>Consolidated Screening List</u>: A list of entities for which the USG maintains restrictions on certain exports, reexports, or items transfers
- System for Award Management (SAM)'s entity exclusions from USG procurement actions; sanctions, restrictions, and prohibitions; and ineligibility to contract with the USG
- Supplier Performance Risk System's company exclusion status for Department of Defense acquisition professionals, including debarments and suspensions

Traceable Company Information Examples

The following data points are generally available in the public domain or via SAM:

Company's Legal Name	Public/Private Status	Company Description	Incorporation Date and Location
Headquarters Address	Stock Ticker Symbol	DUNS Number	Employee Number
Website Address	For Profit/Nonprofit or Academic Status	Unique Entity Identifier	Office Locations

Additional Company Information Considerations

The following data points and questions can augment your due diligence efforts:

Contracting Data Points		Security Clearance Questions	
Number of contracts within [date range]		Does the company participate in the National Industrial	
Dollar amount obligated		Security Program (NISP?)	
		What is the company's	
Specific agencies issuing		Facilities Clearance (FCL) level?	
Presence of company products in subcontracts		What is the company's highest Employee Clearance level?	
l '			

Diving Deeper: Consistency Across Findings

Research may uncover conflicting findings and data points for traceable company information. Consider validating against USG-derived sources and company-derived sources for the most up-to-date information.

Related Resources

- <u>Bloomberg</u> offers publicly available and neutral company descriptions without a sales pitch.
- <u>USASpending</u> and the <u>Federal Procurement Data System (FPDS)</u> contain contracting data.
- <u>SAM.gov</u> and the <u>NISP Central Access Information Security System (NCAISS)</u> contain security clearance data but require specialized permissions to review it.

NIST Due Diligence Assessment Quick-Start Guide:

Due Diligence Research Categories

SUPPLY CHAIN TIERS

Organization of suppliers into levels based on relationship to the end user

Research Considerations

Due Diligence Supply Chain Tiers Definition

- Suppliers are organized into tiers based on their relationship to the end user.
- First-tier suppliers provide products and/or services directly to the end user.
- Second-tier suppliers provide products and/or services to first-tier suppliers.
- The tiers can go down to X level, depending on organizational preference. Going down further in the supply chain tier structure increases one's visibility and understanding, but the difficulty and cost exponentially increase.

Illuminating the Supply Chain Tier Structure with Tools

Researching with supply chain illumination tools can help you visualize the organization or program's supply chain tier structure, identify commonalities and relationships across suppliers, and potentially provide insight into supplier concerns.



Due Diligence Considerations on Supply Chain Tiers

- Supplier presence on regulatory compliance lists, watchlists, or USG exclusion lists (see <u>Stability</u>)
- FOCI concerns with direct and sub-tier suppliers
- Organization-defined concerns with direct and sub-tier suppliers (e.g., foreign defense and aerospace entities that are direct suppliers of programs that support national security systems)

Sub-Tier Supplier Diversity

 The further one gets from the end user, the larger the supplier portfolio becomes, increasing a corresponding likelihood of supplier presence on an exclusion list, watchlist, or regulatory noncompliance list.

Questions to Consider

- Analyzing the supply chain tier structure can illuminate sole source supplier concerns. Do multiple direct suppliers all rely on the same sub-tier suppliers?
- What is your organization's risk tolerance for FOCI concerns with direct and sub-tier suppliers?
- How should your organization's risk tolerance balance the risks of limited supplier diversity with the increased likelihood of watchlisted suppliers in the sub-tier portfolio?

Related Resources

NIST IR 8179, Criticality Analysis Process Model

Link to SP 800-161r1 and Related Resources



Diligence

FOCI

Foreign Ownership, Control, or Influence

Research Considerations

Due Diligence FOCI Definition

• FOCI considerations for a supplier constitute significant ties to governments or government-controlled interests outside of the designated focal country with the power to affect the company's management or operations.

Ownership

• A foreign government holds [organization-defined] significant, ultimate, beneficial, or institutional ownership stake in the supplier, allowing that entity to influence policies and/or organizational or supply chain decisions that the supplier makes.

Key Leadership

• Executive-level leadership and/or supply chain leadership have [organization-defined] significant ties to foreign governments.

Foreign Laws, Policies, and Regulations

- Some nations have legal requirements for entity sharing with their security services, even for products and services that are not under their direct ownership, control, or influence.
- Sharing can encompass intellectual property, source code, design schematics, customer data, or other sensitive proprietary information as a prerequisite for conducting business within the foreign nation.
- Caveat: minimal investigation may extend beyond foreign government OCI into noncommercial entity partnerships, including geopolitical and regulatory relationships.

Key Questions

The following considerations can assist in developing FOCI questions to focus research:

Ownership/Control	
Does this company have foreign ownership, investment, or headquarters?	
Is the company undergoing an impending foreign merger or acquisition?	

Influence	
What SCRM-relevant Key Leaders have ties to foreign governments?	
Is the company subject to laws of sharing and cooperation with foreign security services?	

Levels of Concern can be assigned to Findings based on organization-defined risk tolerance and system criticality.

Diving Deeper: Organization-Defined Parameters

Individual organizations will need to define their own system of trust regarding FOCI elements.

- Which countries are considered low, moderate, or high risk?
- How much foreign exposure can the organization tolerate in its critical suppliers?
- Can FOCI findings of concern be mitigated?

Related Resources

- Department of Commerce Foreign Adversaries List
- Department of State Countries of Concern

PROVENANCE



Place of origin for a supplier's operations or specific product development

Research Considerations

Due Diligence Provenance Definition

- Chronology of the origin, development, ownership, location, and changes to a system or system component, associated data, personnel, and services (SR-4), including analyses of component and subcomponent inventories (e.g., hardware and software bills of materials)
- Note: Per SR-4, *Pedigree* is the validation of provenance with evidence.

Supplier Operational Locations

- Research and development laboratories or locations of key source-code developers
- Manufacturing facilities, including factories and fabrication sites
- Assembly (i.e., where product subcomponents are put together)
- Testing and quality control
- Warehousing and storage (both physical facilities and virtual data servers)
- Shipping, distribution, and logistics nodes (e.g., air, land, and sea transportation)

Product-Specific Locations

- Findings specific to a particular product, component, or subcomponent
- For hardware, publicly available provenance locations at the country level, including manufacturing or assembly locations
- For software, open-source and third-party source code along with proprietary code development
- Third-party vendor or reseller supply chain

Link to SP 800-161r1 and Related Resources

Provenance Research Sources

The following resources can assist in identifying the key locations in a company's supply chain operations or the provenance of an individual product via publicly available information:

Supplier Sources	Hardware Sources	Software Sources	
 Company-derived material (e.g., website, press releases, blog posts, legal policy) Annual <u>Securities and</u> <u>Exchange Commission</u> (<u>SEC</u>) filings 	 Company-provided datasheets Online marketplace listings and product photos 	 Company-provided software license documentation Source-code repositories and binary files (e.g., for open-source software) Software bills of materials (SBOMs) 	

Levels of Concern can be assigned to Findings based on organization-defined risk tolerance derived from the parameters used for FOCI.

Diving Deeper: Subcomponents

- Provenance research also encompasses the supply chain of critical product subcomponents.
- To scope research for hardware, consider whether logic-bearing components store, send, save, assess, or transmit data.
- SBOMs should only be produced using NTIA-supported formats that can satisfy <u>EO 14028</u> minimum elements as framing for the inclusion of primary components. They should be digitally signed using a verifiable and trusted key.
- Subcomponents may be made in one country with a different assembly country being listed as the "country of origin."

Related Resources

<u>NTIA: The Minimum Elements for a Software Bill of Materials</u>

STABILITY

Findings that impact the reliability, regulatory compliance, or authenticity of a supplier or product

Research Considerations

Due Diligence Stability Definition

• Information that potentially impacts the ability of a supplier to meet contractual obligations, including product reliability, supplier compliance with government regulations, and the presence of counterfeit devices in the market space

Organizational Stability Concerns

- Financial distress (e.g., bankruptcies, credit insolvency, significant debt, risky investments)
- Legal difficulties (e.g., significant lawsuits/litigation, particularly those related to product stability; instances of industrial theft or espionage)
- Leadership turnover for key executive positions
- Regulatory violations (e.g., export controls, International Trafficking in Arms, Foreign Corrupt Practices Act, government exclusions)
- Known associations with terrorist or criminal elements
- Data breaches, including ransomware
- Use of conflict materials or forced labor
- Environmental instability in key operational locations

Product Stability Concerns

- Customer reports of poor product performance
- Known instances of counterfeiting or unauthorized white-labeling
- Known instances of a supplier frequently showing willful negligence or deploying intentionally malicious practices that can degrade the customer's level of trust in its products

Regulatory Compliance Lists

The following entities represent various USG prohibitions that may be useful in identifying government exclusions of suppliers or their key personnel:

- FY99 NDAA Section 1237
- FY19 NDAA Section 889
- FY21 NDAA Section 1260H
- FY23 NDAA Section 5949
- FCC's SECURE Networks Act Covered List
- ITA's Consolidated Screening List

Levels of Concern can be assigned to Findings based on organization-defined risk tolerance.

Diving Deeper: Historical Data vs. Relevant Information

Organizations must define their own levels of risk tolerance for the following findings variables:

- Age of the information found
- Frequency of event occurrence
- Severity of finding
- Supplier mitigations currently (or not) in place to prevent reoccurrence

Related Resources

- System for Award Management
- National Vulnerability Database

FOUNDATIONAL CYBER PRACTICES 1



Part 1: Overall cybersecurity posture of a supplier's public-facing information technology assets

Research Considerations

Due Diligence Foundational Cyber Practices: Part 1 — Securing the Supplier

• Findings regarding the cyber health of the supplier's public-facing information technology (IT) assets to measure its ability to deliver on promised services and safeguard sensitive data

System Compromises

- Malware infections, including server and botnet compromises
- Spam propagation (i.e., automated distribution of large amounts of unsolicited communications)

User Behavior

- Exposed credentials from third-party data breaches
- BitTorrent protocol file sharing

Security Posture

- Unnecessary open ports
- Vulnerability patching cadence
- Mobile application security
- Endpoint/configuration security
- Presence of obsolete software versions
- Susceptibility to ransomware attacks or business interruption
- Unwanted functionality

Spotlight on Data Breaches

When assessing the ramifications of a data breach or successful cyber attack against a supplier, consider the following questions:

- How long ago was the incident?
- What did the incident entail, and what was the severity of the impact?
 - For example: Credentials stolen, sensitive data compromised/exfiltrated, denial of service
- What steps did the supplier take to mitigate the attack's impact and prevent future occurrences?

Technical Deep Dive: NIST Computer Security Incident Handling Guide

Where to Find Information

Some aggregated information about public-facing IT assets is not available on the open web and may require the use of an illumination tool for analytics, such as:

- Domain Name Services Checker (<u>DNSChecker</u>) and <u>Robtex</u> provide a basic and open-source overview of a website's metadata.
- Shodan is a search engine for internet-connected devices that can give a footprint of a supplier's network.
- <u>HackerTarget</u> offers multiple free tools for DNS health checks, IP geolocation, port scanning, network tests, and web tools.
- <u>VirusTotal</u> offers malware detection and analysis for URLs, files, domains, and IPs.
- Free Secure Socket Layer (SSL) grading websites like <u>Qualys SSL Labs Scanner</u> or <u>Mozilla</u> <u>Observatory</u> offer analysis for web server SSL configurations.

FOUNDATIONAL CYBER PRACTICES 2



Part 2: Secure product development and product-specific cybersecurity concerns for software and firmware

Research Considerations

Due Diligence Foundational Cyber Practices: Part 2 — Secure Product Development

 Supplier's use of cybersecurity key practices when developing products as well as product-specific concerns that cause offerings to not operate as the manufacturer originally intended, including software and firmware found in hardware products

Publicly Available Product Findings

- Unpatched Common Vulnerability Exposures (CVEs)
- Product lifespan (e.g., end-of-life considerations, cessation of security updates, product maturity)
- Update/upgrade frequency, including latest available product version

SBOM Analytics Findings

- Sole-source committers: Software dependencies or subcomponents that rely on an individual for updates, maintenance, and patches or on a small number of contributors
- Level of community support and engagement for SBOM subcomponents
- Maintenance frequency (i.e., how often the component/dependency sourcecode is revised or updated)
- Subcomponent end-of-life considerations
- Presence (i.e., percentage and analytics) of committers with FOCI concerns
- Presence (i.e., percentage and analytics) of known vs. unknown subcomponents
- Known unpatched and/or exploited CVEs in subcomponents or dependencies
- Note: SBOM analysis of multiple subcomponents is more scalable when done using an SBOM illumination tool.

Secure Development Practices

Secure-by-design tactics, techniques, and procedures (TTPs) include:

- Use of memory-safe programming languages
- Associated hardware that incorporates architectural features to enable fine-grained memory protection
- Incorporation of well-secured software subcomponents (e.g., libraries, modules, middleware, frameworks) from verified developers with validated provenance
- Web template frameworks that implement automatic user input escaping
- Queries parameterized rather than via user input
- Application source-code undergoes static and dynamic security testing as well as code review
- Infrastructure designed so that one security control compromise does not compromise the entire system

Technical Deep Dive: <u>SP 800-218</u>, Secure Software Development Framework

Supplier Software Attestation: Finding Secure Development Practices Information

- Per OMB <u>M-22-18</u> and <u>M-23-16</u>, federal agencies require software developers to attest to following Secure Software Development Framework (SSDF) practices.
- While attestation information may not currently be public-facing, the industry trend is to increase transparency around compliance with secure software development practices.
- Federal employees can access CISA's Repository for Software Attestation and Artifacts (RSAA) <u>here</u>.

Related Resources

- <u>SP 800-160v2r1, Developing Cyber Resilient Systems</u>
- <u>CISA's Secure Software Development Attestation Form</u>

NIST Due Diligence Assessment Quick-Start Guide:

Putting It Together

Due Diligence Findings and Classification

FOCI Provenance Due Diligence Foundational Oyber Practices

Classifying Due Diligence Findings

While this guidance discusses publicly available information and findings that are derived from open-source research or commercially derived datasets in the public domain, organizations need to determine what classification the aggregation of findings and individual findings should hold, if any.

- Findings that aggregate vulnerabilities in information systems for National Security Systems (NSS) and other programs resident on classified systems should follow the appropriate Security Classification Guide for classification markings. For programs that are not resident on NSS or classified systems, consider marking documents that aggregate vulnerability findings as Controlled Unclassified Information (CUI) to protect vulnerability information.
- Consider marking individual findings that are derived from commercial illumination tools or those that require login credentials or special roles/access within government systems as CUI to protect those sources' proprietary business information.

Additional Resources

- The <u>National Archives and Records Administration Controlled Unclassified Information Categories</u> provide federal-level guidance on CUI policies and practices for specific subsets of CUI.
- <u>SP 800-171r3, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations</u>, provides recommended security requirements for protecting the confidentiality of CUI.
- <u>SP 800-161r1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations</u>, provides guidance on identifying, assessing, and mitigating cybersecurity risks throughout the supply chain at all levels of an organization.
- The <u>NIST Cybersecurity and Privacy Reference Tool (CPRT)</u> provides reference data from various NIST cybersecurity and privacy standards, guidelines, and Frameworks in common downloadable formats (e.g., XSLS and JSON).
- SP 800-53r5, Security and Privacy Controls for Information Systems and Organizations, provides a catalog of security and privacy controls for which SP 800-161r1 offers additional enhancements that are specific to C-SCRM. The controls are flexible, customizable, and implemented as part of an organization-wide process to manage risk. View and export information from the Cybersecurity and Privacy Reference Tool (CPRT).

REVIEW: LEARNING RECAP

A Summary of the Key Concepts From This Due Diligence Assessment Quick Start Guide

What We Learned. This Quick-Start Guide explained the following:

- Due diligence in cybersecurity supply chain risk management (C-SCRM) The process of researching and verifying available information about a given ICT supplier or product prior to entering into an agreement
- Supply chain risk assessments (SCRA) Assessments of cybersecurity risks that arise from business partners seeking to integrate with a given system
- Due diligence research considerations First Steps (pre-checks and traceable company information); Supply Chain Tiers (organizing suppliers into levels based on their relationship to the end user); Foreign Influence, Control, or Ownership (FOCI); Provenance (place of origin for the supplier's general operations or a specific product); Stability (findings that impact the reliability, regulatory compliance, or authenticity of a supplier or product); and Foundational Cyber Practices (overall cybersecurity posture of a supplier's public-facing information technology assets and cybersecurity concerns for hardware, software, and product development) to ensure that informed decisions can be made about whether to enter into contracts and agreements.

What's Next. Here are two things you can do to move this QSG into practice:

- **1. Develop a Due Diligence Report template** that includes findings for research and sources to find and verify information (both PAI and commercially provided).
- 2. Define levels of concern for findings. Use your organization's baseline risk tolerance to develop a rating schema that determines when findings rise to a level of concern that constitutes risk.

This QSG provides an overview of C-SCRM due diligence. It is a supplement to SP 800-161r1 and is not intended to replace it.

New to C-SCRM?

These NIST resources can help you understand the basics of C-SCRM and complete your due diligence assessments:

- NIST's <u>Cybersecurity SCRM Fact Sheet</u> provides a brief but substantive introduction to C-SCRM.
- SP 800-161r1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations, helps organizations identify, assess, and respond to supply chain risks at all levels. It is flexible and builds on the organization's existing cybersecurity practices. Appendix A identifies the C-SCRM-related controls from SP 800-53r5, augments those controls with additional supplemental guidance, and provides new controls as appropriate.
- <u>SP 1305, Cybersecurity Framework 2.0 C-SCRM Quick Start Guide</u>, offers guidance on establishing a C-SCRM capability and using the CSF to communicate supplier requirements.
- The <u>Federal C-SCRM Forum</u> fosters collaboration and the exchange of C-SCRM information among federal organizations to improve the security of federal supply chains.
- The <u>Software and Supply Chain Assurance Forum</u> provides a venue for government, industry, and academic participants from around the world to share their knowledge and expertise regarding C-SCRM, supply chain risks, effective practices and response strategies, tools and technologies, and any gaps related to the people, processes, or technologies involved.

GLOSSARY

Definitions of Key Terms From This Due Diligence Assessment Quick-Start Guide

The definitions in this glossary are meant to inform research in the context of C-SCRM and due diligence. They are not intended to be used as holistic, stand-alone definitions outside of that context.

- **Basic due diligence:** Desktop-based research using open sources and publicly available information (PAI) to derive due diligence findings.
- **Due diligence:** The investigative process of researching and verifying available information about a given supplier or product prior to entering into an agreement so that informed decisions can be made with all available and pertinent information.
- Enhanced due diligence: The use of commercial datasets, proprietary sources, and supply chain illumination tools to derive due diligence findings.
- Foreign ownership, control, or influence (FOCI): Significant ties to governments or government-controlled interests outside of the designated focal country with the power to affect a company's management or operations.
- Provenance: Chronology of the origin, development, ownership, location, and changes to a system or system component, associated data, personnel, and services (SR-4), including analyses of component and subcomponent inventories (e.g., hardware and software bills of materials).
- **Stability:** Information that potentially impacts the ability of a supplier to meet contractual obligations, including product reliability, supplier compliance with government regulations, and the presence of counterfeit devices in the market space.

NIST CSRC Glossary

NIST's Computer Security Resource Center (CSRC) contains a glossary that aggregates terms and definitions specified in NIST's cybersecurity and privacy standards, guidelines, and other technical publications, as well as other official sources, including U.S. laws, the Code of Federal Regulations, Presidential Directives, and the Committee for National Security Systems.

Users of this Quick-Start Guide may consult the CSRC Glossary for variations of these terms that may exist in other contexts.

The Glossary is available <u>https://csrc.nist.gov/glossary</u>.