Cybersecurity Supply Chain Risk Management (C-SCRM) Acquisition Guide

April 2025

Version 1.1

Cybersecurity Supply Chain Risk Management (C-SCRM) Acquisition Guide

Document Revision History

Revision Number	Revision Date	Summary of Changes	Author
1.0	7/14/2023	Initial document creation	MetaPhase Consulting (MPC)
1.1	4/1/2025	Removed DEI references	Cybersecurity Information Assurance and Privacy (CIAP) Branch

Contents

Executive Summary

This Cybersecurity Supply Chain Risk Management (C-SCRM) Guide (referred to as the Guide) is meant to assist federal, state, local, tribal, and territorial government departments and agencies (collectively referred to as "agencies") in the acquisition of C-SCRM tools and advisory services currently available on General Services Administration (GSA) contract vehicles.

The Guide describes some of the key capabilities, components, and features of commercial C-SCRM illumination and supply chain risk assessment (SCRA) tools and their use by agencies throughout the acquisition life cycle. The document also provides some considerations for C-SCRM technical advisory services that could support a wide range of C-SCRM activities for agencies. The Guide also provides information on how these tools and services:

- Address key legislative and regulatory requirements, directives, and National Institute of Standards and Technology (NIST) guidance;
- Support government C-SCRM activities described in relevant security control families and controls in NIST Special Publication (SP) 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations* (NIST SP 800-53r5) and NIST SP 800-161 Revision 1, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations* (NIST SP 800-161r1); and
- Address various risks third-party suppliers, and the products and services provided by those suppliers, can pose to agencies' systems and networks.

This Guide summarizes and excerpts a substantial amount of information directly from NIST SP 800-161r1. The NIST guidance is the best source of detailed information on how government agencies should implement controls, practices, and policies to effectively address cybersecurity risks arising from the supply chain.

Finally, the Guide identifies GSA contract vehicles through which government agencies can acquire existing C-SCRM tools and services and describes best practices for incorporating C-SCRM tools and services requirements into a Request for Information (RFI), Request for Proposal (RFP), Request for Quote (RFQ), Statement of Objectives (SOO), Sources Sought Notice (SSN), Performance Work Statement (PWS), or Statement of Work (SOW) for future procurements.

Cybersecurity Supply Chain Risk Management Drivers

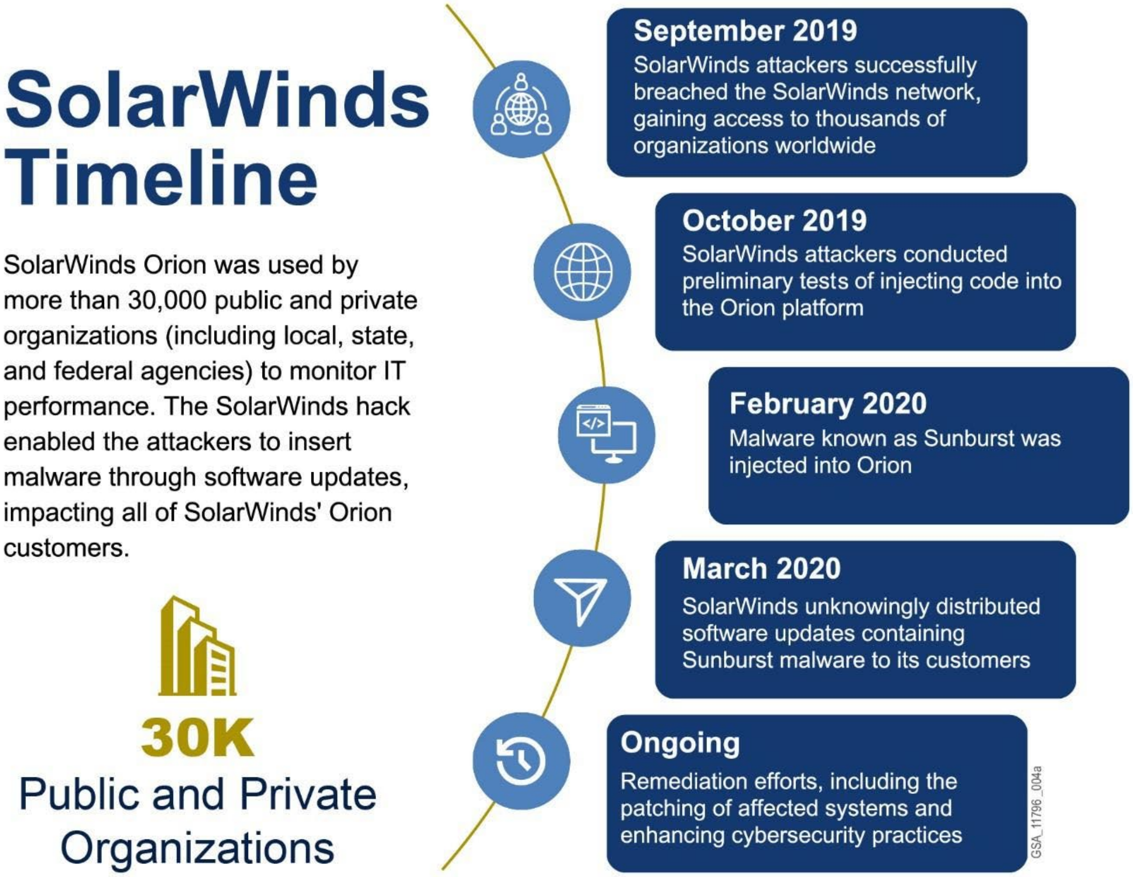
High Impact Supply Chain Incidents

For this Guide, C-SCRM tools are defined as those manual or automated tools that provide access to data and analyses that informs government agencies about suppliers, their associated supply chains, and the risks that may be inherited by the government related to the acquisition and use of Information and Communications Technology (ICT) and Operational Technologies (OT). In accordance with the terminology and definitions used in NIST SP 800161r1, ICT includes covered articles[1] as well as all ICT products (hardware and software) and services; OT includes products and services related to the Internet of Things (IoT). Like NIST SP 800-161r1, this Guide will refer to those technologies (products and services) collectively as ICT/OT.

ICT/OT supply chains are subject to a variety of cybersecurity and other disruptive risks. Threats to the supply chain are constantly growing in sophistication, number, and diversity. These threats may affect the confidentiality, integrity, or availability of government information and information systems and include counterfeiting, tampering, theft, reduced or unwanted functionality, or malicious content. These threats may be intentional or unintentional, but any of them could significantly impact the security, resilience, safety, etc. of the organization and its stakeholders. Unintentional threats include “inadequate or poor product security and integrity practices throughout the development life cycle; unintended access to critical systems; poor procurement standards and practices; reliance on third-party providers for subcomponents; and inadequate personnel screening.”[2] Vulnerabilities that can be exploited to enable these threats may be instantiated by adversarial or malicious individuals, organizations, or nation-states or because of a lack of good processes and practices throughout the development life cycle.

Disruptions and attacks on ICT/OT supply chains have been increasing in frequency and scale. Examples include the following:

- The SolarWinds hack enabled attackers to insert malware through software updates, impacting all of SolarWinds’ Orion customers. SolarWinds Orion was used by more than 30,000 public and private organizations (including local, state, and federal agencies).
- Ransomware distributed through software provider Kaseya to end-customer systems which affected over 1,500 organizations
- Zero-day vulnerabilities in Microsoft Exchange which were exploited and used to compromise over 18,000 organizations worldwide
- Global disruptions resulting from COVID-19 restrictions and workforce availability
- Weather events such as hurricanes, tsunamis, ice storms, and tornadoes.



SolarWinds Timeline

SolarWinds Orion was used by more than 30,000 public and private organizations (including local, state, and federal agencies) to monitor IT performance. The SolarWinds hack enabled the attackers to insert malware through software updates, impacting all of SolarWinds' Orion customers.

30K Public and Private Organizations

September 2019
SolarWinds attackers successfully breached the SolarWinds network, gaining access to thousands of organizations worldwide

October 2019
SolarWinds attackers conducted preliminary tests of injecting code into the Orion platform

February 2020
Malware known as Sunburst was injected into Orion

March 2020
SolarWinds unknowingly distributed software updates containing Sunburst malware to its customers

Ongoing
Remediation efforts, including the patching of affected systems and enhancing cybersecurity practices

Figure 1. Timeline Showing the Attack of SolarWinds Orion

C-SCRM Requirements

The increase in frequency and impact of supply chain disruptions and incidents led directly to numerous legislative and executive actions in the last ten years. Federal executive branch agencies are now mandated to implement C-SCRM practices based on NIST standards and guidance and may choose to support their in-house capabilities by acquiring commercial off-the-shelf (COTS) C-SCRM tools and services. These tools must have the capabilities needed to comply with externally driven priorities (e.g., governmentwide policy direction, regulatory requirement, etc.) and agency-specific defined needs (e.g., prioritization factors). Some of the major legislative, executive, and regulatory actions that direct agencies to improve the management of their supply chain cybersecurity risks include the following:

- The Federal Acquisition Supply Chain Security Act of 2018 (FASCSA): Title II of the Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure (SECURE) Technology Act and the ensuing rule of the Federal Acquisition Security Council (FASC), which was created to implement the legislation, requires all federal agencies have a C-SCRM program and that agencies prioritize, assess, avoid, mitigate, accept, or transfer supply chain risks. FASCSA also aims to improve executive branch coordination, supply chain risk information sharing, and actions to address supply chain risks.

- Section 889 of the National Defense Authorization Act (NDAA) for Fiscal Year 2019: Section 889 prohibits executive agencies from entering into a contract (or extending or renewing a contract) with any entity that uses telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation, and video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities). It also extends the prohibition to the sub-tier suppliers, highlighting the criticality of understanding who is in the agencies' supply chains.
- Executive Order (EO) 13873 (*Securing the Information and Communications Technology and Services Supply Chain*, May 15, 2019), EO 14017 (*Executive Order on America's Supply Chains*, February 24, 2021), EO 14028 (*Executive Order on Improving the Nation's Cybersecurity*, May 12, 2021), and EO 14034 (*Executive Order on Protecting Americans' Sensitive Data from Foreign Adversaries*, June 9, 2021): These EOs collectively recognize the need for federal executive branch agencies to address risks associated with the ICT supply chains to help protect national security interests.
- Office of Management and Budget (OMB) Circular A-130 *Managing Information as a Strategic Resource*: This outlines how agencies should protect information, to include specific guidance and requirements around ICT SCRM.
- Committee on National Security Systems (CNSSD) No. 505 *Supply Chain Risk Management (SCRM)*: This document assigns responsibilities and establishes the minimum criteria for the continued development, deployment, and sustainment of a SCRM program (or capability) for the protection of National Security Systems (NSS) or non-NSS that directly support NSS. This includes connections to and dependencies on cyber-physical, system-of-systems, and outsourced IT services or other critical information sources or functionality required for the success of NSS supported missions.
- OMB Memorandum M-22-18 and its update OMB Memorandum M-23-16: Consistent with directives in EO 14028, these require that federal agencies only use software provided by software producers who attest to complying with government-specified secure software development practices, as described in the NIST Secure Software Development Framework (SSDF) SP 800-218 and the NIST Software Supply Chain Security Guidance. Prior to using any purchased software, agencies are required to obtain a self-attestation from the software producer, which indicates that they have implemented the NIST guidelines during the software's development.
- Federal Information Security Modernization Act of 2014 (FISMA): Agencies are required to report on their C-SCRM performance on a quarterly and annual basis. The FY 2023/2024 Inspector General (IG) FISMA reporting metrics assess agencies' C-SCRM performance and maturity based on four measurements, two of which explicitly focus on an agency's ability to ensure that products, system components, systems, and services of external providers are consistent with the agency's cybersecurity and supply chain requirements, as well as that counterfeit components are detected and prevented from entering the agency's systems.
- Federal Acquisition Regulation (FAR): The FAR is the primary regulation for use by all executive agencies in their acquisition of supplies and services with appropriated funds.

The FAR contains several requirements related to C-SCRM, as do several of the agency-specific FAR supplements (e.g., the Defense Federal Acquisition Regulation Supplement (DFARS)) and the National Aeronautics and Space Administration (NASA) FAR Supplement (NFS)). The Federal Acquisition Regulatory Council (FAR Council) is establishing FAR part 40, which will be the new location for cybersecurity supply chain requirements in the FAR. This new FAR part will provide contracting officers with a focused location in the FAR for cybersecurity supply chain risk management requirements.

Audience

The Guide is intended for professionals with various roles related to C-SCRM, including but not limited to acquisition personnel, mission and business owners, and system owners. Basic knowledge of C-SCRM practices and familiarity with NIST SP 800-161r1 and SP800-53r5 is recommended.

Cybersecurity Supply Chain Risk Management

The Challenge with the Globally Distributed Nature of Technology

ICT/OT relies on a complex, globally distributed, extensive, and interconnected supply chain ecosystem that consists of geographically diverse routes, a constantly changing technology and business environment, and multiple levels of outsourcing. This complexity makes it increasingly difficult for the buyers of ICT/OT to have insight into how the products and services they procure are designed, developed, manufactured, assembled, delivered, and disposed; or whether the processes, procedures, standards, and practices their suppliers use to ensure the security, resilience, reliability, safety, integrity, and quality of those products and services resulting in significant cybersecurity risks are adequate.

Government agencies rely heavily on COTS ICT/OT products, external system integration and support for custom-built systems, and external service providers to carry out their missions. Incorporating COTS hardware and software into its networks and systems permits the federal government to leverage state-of-the-art innovation without bearing the cost of research and development. While the benefits are substantial, there are also consequences of such reliance on COTS products that affect the federal government’s ability to protect information and information systems.

Cybersecurity Supply Chain Risks

Cybersecurity supply chain risks refer to the potential for negative impacts that arise from the exploitation of vulnerabilities in suppliers, their supply chains, or their cyber-related products or services. Cybersecurity risk in an agency’s supply chain may lead to harm on its missions, ranging from a reduction in service levels leading to customer dissatisfaction to the theft of intellectual property or the degradation of critical mission and business processes. These risks can be associated with agencies’ lack of visibility into and understanding of how the products and services they acquire are developed, integrated, and deployed or the processes, procedures, standards, and practices used to ensure the products and services' security. This lack of visibility is depicted in Figure 2, a diagram that was initially shared in NIST SP 800161r1. Some examples of how cybersecurity threats can be introduced into the supply chains include:

- Counterfeit products or components
- Hardware or software delivered with malware
- Malware inserted post-delivery while being serviced
- Hardware or software with unwanted or undocumented functionality
- Vulnerabilities in systems and networks used by supply chain partners
- Insider threats (including non-adversarial)
- Poor quality manufacturing, development, maintenance, or disposal practices
- Supply chain disruptions
- Theft or alteration of system data.

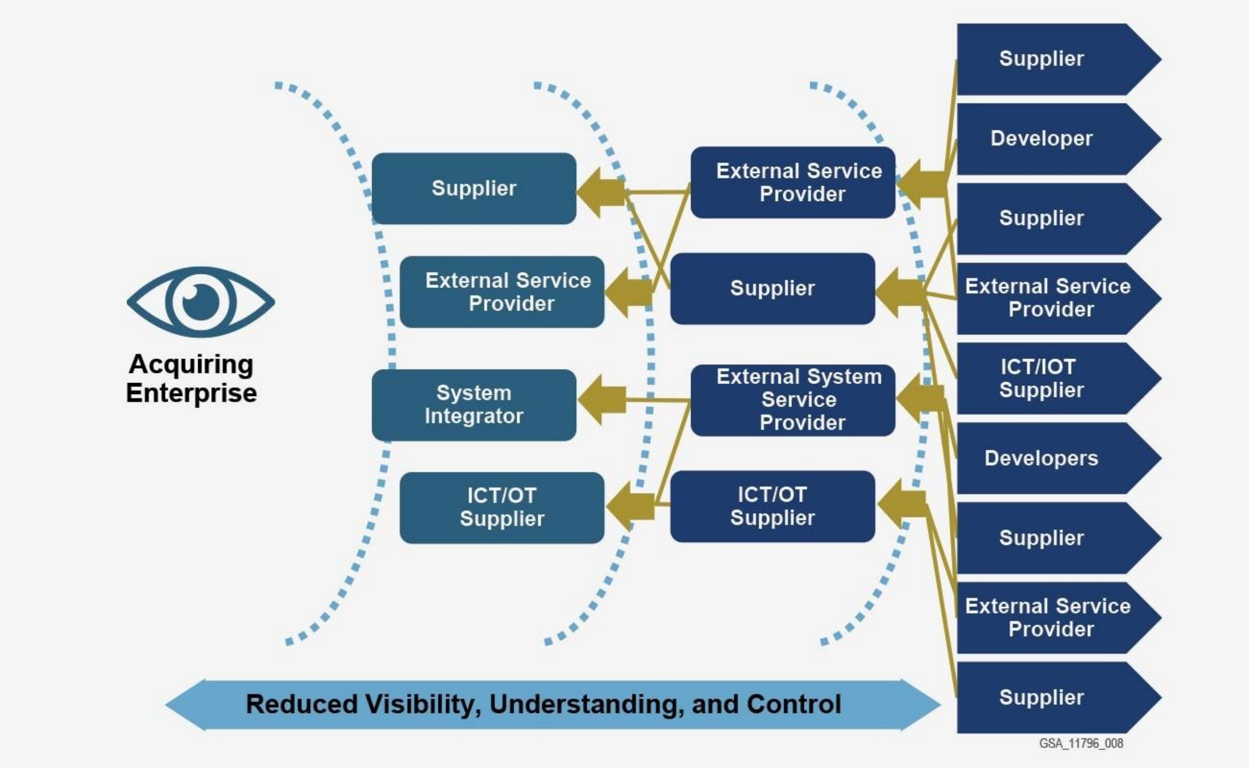

Acquiring Enterprise
Supplier
External Service Provider
System Integrator
ICT/OT Supplier
External Service Provider
Supplier
External System Service Provider
ICT/OT Supplier
Supplier
Developer
Supplier
External Service Provider
ICT/IOT Supplier
Developers
Supplier
External Service Provider
Supplier
Reduced Visibility, Understanding, and Control
GSA_11796_008

Figure 2. An Enterprise's Visibility, Understanding, and Control of its Supply Chain

Managing Risk in ICT Supply Chains

NIST SP 800-161r1 provides guidance to public and private sector entities on identifying, assessing, and responding to cybersecurity risks throughout their supply chain at all levels of their organization, as depicted in Figure 3. NIST defines C-SCRM as a "systematic process for managing exposure to cybersecurity risks throughout the supply chain and developing appropriate response strategies, policies, processes, and procedures."

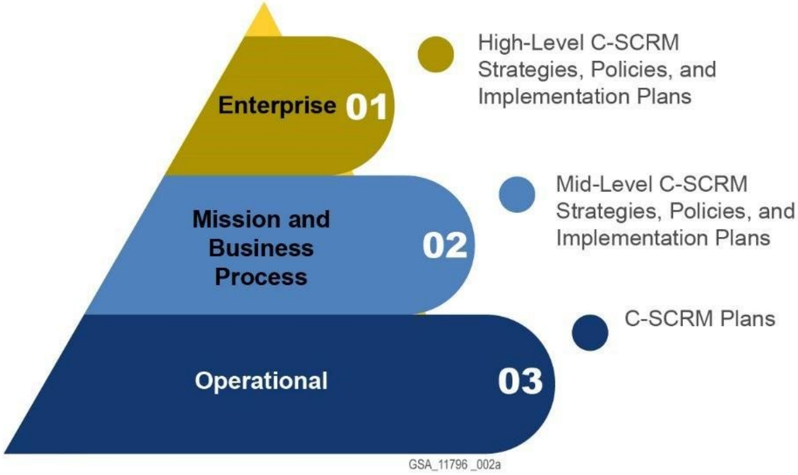
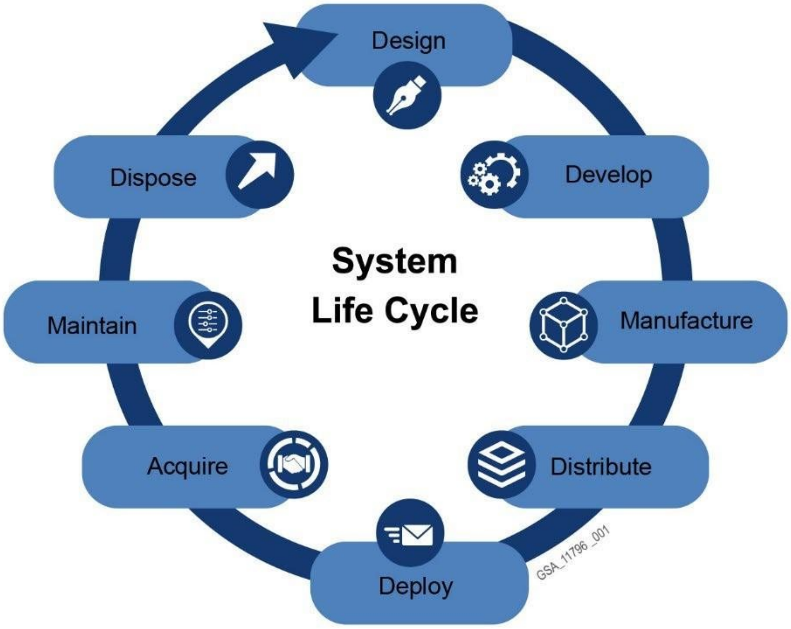

Enterprise 01
High-Level C-SCRM Strategies, Policies, and Implementation Plans
Mission and Business Process 02
Mid-Level C-SCRM Strategies, Policies, and Implementation Plans
Operational 03
C-SCRM Plans
GSA_11796 _002a

Figure 3. Multilevel Enterprise-Wide Risk Management

C-SCRM should cover the entire life cycle of a system (including design, development, manufacturing, distribution, deployment, acquisition, maintenance, and disposal) as supply chain threats and vulnerabilities may intentionally or unintentionally compromise ICT/OT at any stage of the life cycle (Figure 4).



.

Figure 4. System Life Cycle

Supply Chain Risk Assessments

Purpose of Supply Chain Risk Assessments

An important process in C-SCRM is the execution of cybersecurity SCRAs. Agencies perform SCRAs to identify and evaluate the supply chain related risks that arise from using technology products and services. The goal of a cybersecurity SCRA is ultimately to mitigate risks by addressing potential vulnerabilities that could be exploited by cyber attackers to compromise the confidentiality, integrity, and/or availability of agencies' data, systems, and networks. NIST SP 800-161r1 identifies five components of SCRAs, found in Figure 5.

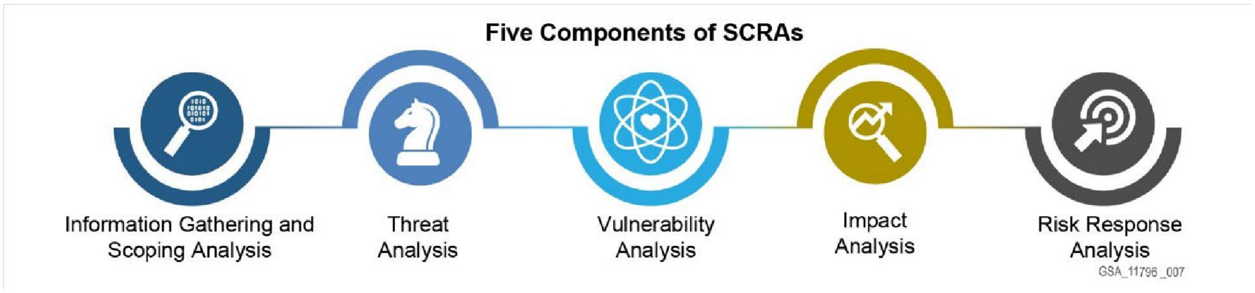


Figure 5. Five Components of SCRAs

SCRAs are also required by FASCSA and other regulatory and executive actions. Agencies should conduct SCRAs prior to the acquisition or use of hardware, software, cloud services, and other technology-related services regularly throughout the system life cycle of those products and services, and in case of a change in the risk environment (e.g., an incident, disruption, or change in regulation or guidance). Agencies should perform SCRAs primarily to mitigate risks to their critical missions and sensitive data within their operational context, not simply to comply with mandates and regulatory requirements. Note that even the service providers and tool providers that can support SCRAs should be assessed for cybersecurity supply chain risks.

Pre-Acquisition Planning Stage

Government mission and business process owners acquiring the product/service, in collaboration with the contracting officer (CO) or contracting officer representative (COR), should:

1. Perform market analysis (e.g., RFI, SSN, market survey) based on an understanding of the need for and criticality of the goods or service to be procured, to identify known sources of supply (including qualified integrators or suppliers and qualified product lists) and begin defining selection criteria and C-SCRM requirements (information can also be gathered from sources such as the press, internet, periodicals, and fee-based services).
2. Conduct due diligence research on potential suppliers and/or products and services using responses to questionnaires and RFIs from potential suppliers and commercial C-

SCRM tools for the initial screening and collection of evidence from potential suppliers during market analysis.

3. Evaluate bidders (i.e., suppliers responding to RFPs or RFQs) against relevant C-SCRM evaluation criteria and conduct robust SCRAs during the solicitation phase. The assessment criteria should include information about the supplier, its security processes, and its security track record. Prior to purchase, agencies should also assess the quality of the product or system components, vulnerabilities, authenticity, and other relevant risk factors and complete the risk assessment prior to deployment. Agencies should select those bids that offer the best value (not merely the lowest cost), considering all documented evidence (e.g., supplier's demonstrated performance and their past performance for same or similar contracts) and the supplier risk assessment.

FASCSA provides agencies the authority to restrict suppliers and their products and services from acquisition and use if it is determined that there is a significant supply chain risk in a procurement (see details, requirements, and limitations in 41 USC 4713).

Post-Acquisition Monitoring

Mission and business owners should monitor risks based on the criticality of the supplier and its product or service. Triggers for conducting an SCRA include the following:

- New suppliers or products/services, such as a supplier adding a new supplier, product, or service to its own supply chain
- Changes in market conditions, such as economic downturns, geopolitical instability, natural disasters, or other market disruptions can impact the supply chain
- A disruption, incident, or cybersecurity breach involving the supplier or a similar supplier or competitor
- Technology changes or advances, such as the adoption of blockchain, artificial intelligence (AI), or IoT
- Changes in regulatory requirements or compliance standards

Assessments of Suppliers, Products, and Services

Agencies conduct analyses and assessments at the mission and systems levels in order to increase their visibility into their critical suppliers, products, and services. A C-SCRM program management office (PMO) or team may assist other agency programs in developing SCRAs before entering those programs into a contractual agreement to acquire products or services. An agency's enterprise-level C-SCRM strategy and policies may place SCRA requirements on programs seeking to acquire products and services. SCRA guidance in NIST SP 800-161r1 provides a step-by-step guide for business partners to follow in preparation for an assessment of suppliers by the C-SCRM PMO. A sample SCRA process flow is found in Figure 6, showing when the process may be initiated and how information is collected and aggregated, leading to a risk assessment and monitoring of the risk environment. Mission-level or program-level policy defines what integration activities require an SCRA. The process and requirements are defined in the SCRA Standard Operating Procedure. The C-SCRM PMO may use all-source information when conducting SCRAs.

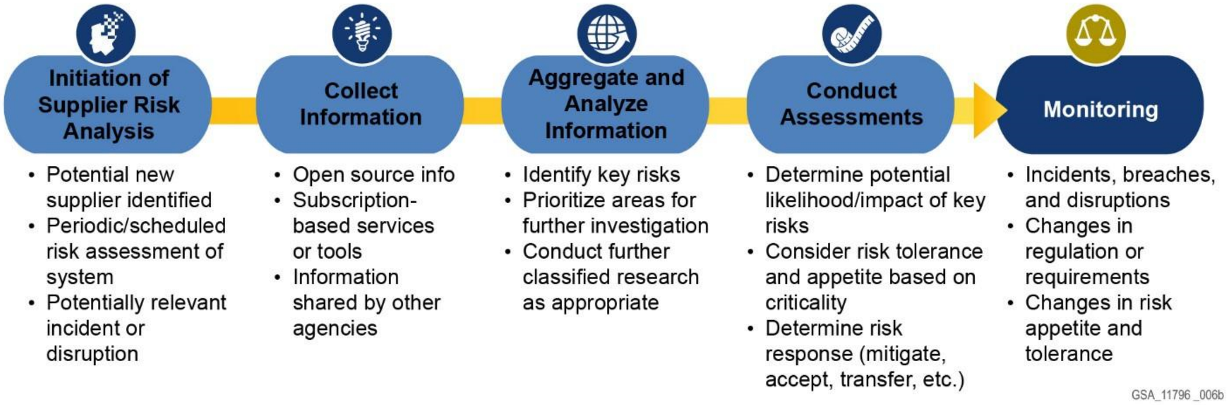

Initiation of Supplier Risk Analysis
• Potential new supplier identified
• Periodic/scheduled risk assessment of system
• Potentially relevant incident or disruption
Collect Information
• Open source info
• Subscription-based services or tools
• Information shared by other agencies
Aggregate and Analyze Information
• Identify key risks
• Prioritize areas for further investigation
• Conduct further classified research as appropriate
Conduct Assessments
• Determine potential likelihood/impact of key risks
• Consider risk tolerance and appetite based on criticality
• Determine risk response (mitigate, accept, transfer, etc.)
Monitoring
• Incidents, breaches, and disruptions
• Changes in regulation or requirements
• Changes in risk appetite and tolerance
GSA_11796 _006b

Figure 6. SCRA Process Flow

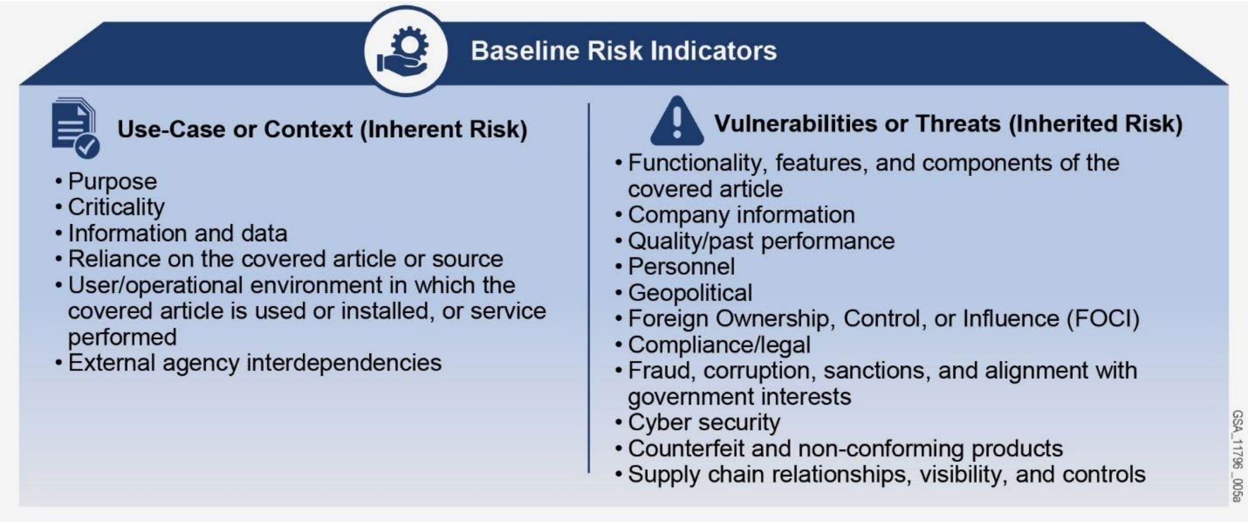
Agencies should consider any information on the supplier that is pertinent to their trustworthiness; this could include information about the security, integrity, resilience, quality, and environmental aspects of their services or products or of the processes and practices used throughout the supply chain. As described in Appendix E of NIST SP 800-161r1, while there are certain SCRA functions that are inherently governmental functions where the accountability and ultimate responsibility should not be outsourced (e.g., prioritizing SCRAs, evaluating impact, making risk response decisions, and taking actions based on the findings in an SCRA), agencies can and typically do acquire advisory services or commercially available data/tools for their supplier and product assessments. Qualified technical advisory contract support can help agencies analyze suppliers, document findings, and review relevant information with appropriate requirements in place to safeguard classified or sensitive supply chain risk information.

NIST SP 800-161r1 also describes how information used for an assessment is comprised of up to three categories of inputs:

1. Purpose and context information (i.e., use-case specific) used to understand the risk environment and to inform and establish risk tolerance relative to the use case
2. Data or information obtained from the supplier
3. All-source information, which may come from publicly available data, government sources (may include classified sources), and/or commercial fee-based sources.

The NIST guidance also notes that the purpose and context, as well as when an assessment of a supplier and/or covered article is performed in the secure development life cycle (SDLC) or procurement life cycle, will drive variations in terms of focus and scope regarding what type, how much, and from what sources of information used in an assessment is obtained.

Agencies should consider applying this information against a consistent set of core baseline factors and assessment criteria based on agencies' risk tolerance and appetite. Each agency can use the risk factors listed and described in SP 800-161r1, Table E-1 to inform the development of their own risk-based assessment criteria. These NIST baseline risk indicators are shown in Figure 7.



Baseline Risk Indicators

Use-Case or Context (Inherent Risk)

- Purpose
- Criticality
- Information and data
- Reliance on the covered article or source
- User/operational environment in which the covered article is used or installed, or service performed
- External agency interdependencies

Vulnerabilities or Threats (Inherited Risk)

- Functionality, features, and components of the covered article
- Company information
- Quality/past performance
- Personnel
- Geopolitical
- Foreign Ownership, Control, or Influence (FOCI)
- Compliance/legal
- Fraud, corruption, sanctions, and alignment with government interests
- Cyber security
- Counterfeit and non-conforming products
- Supply chain relationships, visibility, and controls

Figure 7. Baseline Risk Indicators

Depending on the specific context and purpose for which the assessment is being conducted, agencies may select additional factors. Agencies are cautioned regarding the quality of information (e.g., relevance, completeness, accuracy, etc.) relied upon for an assessment; agencies are recommended to document reference sources for assessment information and verify the information as appropriate.

Information about these baseline risk factors should be generally available from open sources, although the type, quality, cost, and extent of information is likely to vary. Findings associated with these factors may reflect a mix of subjective and objective information regarding threats, vulnerabilities, or general "exposures" that, when assessed discretely or in aggregate, indicate risk being possible or present. Government buyers of C-SCRM tools and services may choose to acquire more than one tool to obtain the needed data and analyses, as no one tool currently provides a comprehensive set of information that addresses all baseline risk.

COTS Supply Chain Risk Assessment Data and Tools

There is an increasing number of companies that offer third-party risk management tools through their Software as a Service (SaaS) platforms using AI and machine learning (ML) solutions; however, currently these tools address only a subset of the baseline risk indicators listed in Table E-1 in NIST SP 800-161r1 and do not provide holistic C-SCRM capabilities. This is partially due to the lack of publicly available information regarding some of the risk factors due to the proprietary or privacy-related nature of the information. In some cases, the information is simply not published anywhere that is accessible to those tools.

SCRA tools and C-SCRM advisory services (people, processes, and technologies), for the purpose of the Guide, consist of capabilities that agencies can use to manage their supply chain risks and typically do not include traditional information security capabilities. The overwhelming majority of controls in NIST SP 800-53r5 are traditional information security controls that can be implemented with C-SCRM considerations (especially with supplemental guidance provided in NIST SP 800-161r1) by the same information security professionals that have been responsible for the implementation of those controls. Those professionals may not require a specific C-SCRM capability to implement them but may benefit from training or experience.

Agencies also need to be aware that vendors that provide C-SCRM tools and services and customers often use different terminology for their products and services. For example, some C-SCRM tool vendors distinguish between C-SCRM and third-party risk management solutions, whereas NIST SP 800-161r1 uses those terms interchangeably. C-SCRM tool providers may refer to their tools and services as supply chain illumination, supply chain visibility, supply chain risk assessment, supply chain risk management, third-party risk management, vendor due diligence, vendor risk management, supply chain resilience, etc., with the intended definition of these terms overlapping or slightly differing. Furthermore, there is no agreed-upon terminology and definition for C-SCRM tools and services among agencies either, which can hinder vendors' ability to develop C-SCRM solutions tailored to agencies' needs or efforts to find specific tools in the marketplace.

These tools can provide agencies with one or more of the following capabilities:

Supply Chain Illumination/Visibility Capabilities

- Identifying potential or probable supply chain connections to suppliers. These connections may be supplier-customer relationships directly related to the product or service being provided or may be related to other products or services provided by the supplier or to indirect relationships like providing office furniture or supplies. These connections could include parent-child or sibling relationships with umbrella companies, subsidiaries, or affiliates. These connections could be business partnerships or other types of relationships. It should be noted that the nature of the identified relationships is often difficult to ascertain or verify.
- Mapping a supplier's supply chain from design and development to the manufacturing of components and systems, from delivery to deployment and system integration of the technologies, and from sustaining and maintenance services to end of life disposal. The information at each tier may not be readily available due to the proprietary nature of the information and may require suppliers at each tier to provide some of that information. It should also be noted that it is often difficult to verify the accuracy or timeliness of that information.
- This type of information can identify potential connections with banned entities (e.g., Section 889).

Supplier Risk Assessment Capabilities

- Identification and assessment of supplier risks related to the location of the supplier's facilities and operations (headquarters, development facilities, manufacturing facilities, logistics hubs, etc.), as well as the logistical routes used to move components and products (these risks can be very dynamic and typically need to be monitored) such as:
  - Weather events (tsunamis, hurricanes, earthquakes, ice storms, etc.
  - Geopolitical issues
  - Potential labor issues
  - Climate impact
  - Epidemics/pandemics
- Identification and assessment of potential supplier risks associated with foreign ownership, control, and influence (FOCI)
- Identification and assessment of supplier risks associated with financial stability, mergers and acquisitions, etc.
- Identification and assessment of supplier risks associated with their internal security and integrity practices (cybersecurity protections, known vulnerabilities, insider threat program, anti-counterfeit measures, etc.)
- Identification and assessment of supplier risks associated with the quality of their products and processes
- Identification and assessment of supplier risks associated with their resilience practices that enable them to continue performing to expectations despite disruptions and incidents.

Product and Services Risk Assessment Capabilities

- Product testing/verification tools can help agencies evaluate and verify that a product or application they purchase functions as expected and does not contain unexpected functionality.
- Determination on whether the product (hardware and software) or service that is being procured is designed, developed, manufactured, and delivered with appropriate security controls to ensure confidentiality, integrity, and availability of information systems and data.
- Tools to assist agencies with asset detection and inventorying and vulnerability management activities, such as analyzing component inventories (Software Bills of Materials (SBOMs) and Hardware Bills of Materials (HBOMs), etc.) for Known Exploited Vulnerabilities (KEVs) and other common vulnerability exposures (CVEs).

-For example, there are commercially available tools that help agencies create SBOMs and HBOMs as well as tools to ingest, analyze, and act on the data contained in SBOMs, HBOMs, software development attestations, and vulnerability advisory reports, which can track the origin, development, ownership, location, and changes to a product, product vulnerabilities, and associated data (provenance).

It may be helpful to map the C-SCRM tools and services to NIST SP 800-53r5 and NIST SP 800-161r1. NIST SP 800-53r5 is a publication of information security and privacy controls for organizations and their information systems. It addresses aspects of C-SCRM throughout relevant controls and introduces a new control family dedicated to Supply Chain Risks (SR). Other control families and controls have been updated to include relevant C-SCRM considerations, for example the Risk Assessment (RA) control family. NIST SP 800-161r1 provides guidance on many distinct aspects of managing risk in supply chains. It should be noted that while the publication provides C-SCRM specific guidance and tools, it also includes an "enhanced overlay" with C-SCRM guidance on top of NIST SP 800-53r5's security and privacy controls. Some C-SCRM specific controls that supply chain risk illumination tools support include those depicted in Figure 8:

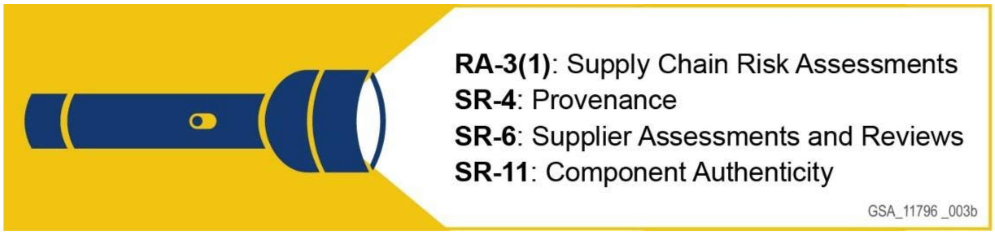

RA-3(1): Supply Chain Risk Assessments
SR-4: Provenance
SR-6: Supplier Assessments and Reviews
SR-11: Component Authenticity
GSA_11796 _003b

Figure 8. Example C-SCRM Control Families

Supply Chain Risk Illumination Tools Available on GSA Contract Vehicles

Agencies can leverage GSA technology purchasing programs when looking for C-SCRM specific and/or related products, services, and solutions with additional requirements to meet their C-SCRM needs. These include:

Multiple Award Schedule (MAS):

- Highly Adaptive Cybersecurity Services (HACS) Special Item Number (SIN) 54151HACS[4]
- Identity, Credential, and Access Management (ICAM) Tools SIN 541519ICAM
- Continuous Diagnostics and Mitigation (CDM) Tools (note that the former CDM Tools SIN retired in 2022, but these tools are now available through the Best-in-Class IT Hardware and Software SINs).
- Mobile Identity Management SIN 517312
- IT Professional Services SIN 54151S
- Data Breach Response & Identity Protection Services (IPS) SIN 541990IPS
- Risk Assessment and Mitigation Services SIN 541990RISK.

Governmentwide Acquisition Contracts (GWACs):

- Alliant 2
- Veterans Technology Services (VETS) 2
- 8(a) Streamlined Technology Acquisition Resource for Services (STARS) III.

For more detail on these contracts, visit the GSA Cybersecurity Supply Chain Risk Management Guide.

There are vendor cybersecurity posture assessment, products and services assessment, and supplier assessment tools and analytic products currently available on GSA contract vehicles that agencies can procure either directly from the tool or service provider or through an authorized distributor, integrator, or partner. These products and services may aid agencies' efforts in the identification and management of their cybersecurity supply chain risks. Many of these vendor offerings leverage automation (to include AI and ML), enabling agencies to take advantage of state-of-the-art information collection and aggregation technologies and capabilities without having to dedicate scarce resources to accomplish similar outcomes.

This section of the Guide provides a list of some key vendors that currently offer third-party risk management solutions on GSA contract vehicles. This is not a comprehensive list of all C-SCRM tools and services providers; there are other COTS C-SCRM tools and services that are available through direct contracting or other non-GSA contract vehicles. Supplemental information on these tools and providers may be found in Appendix C. This is representative of the types of capabilities that are available, and they are listed by vendor in alphabetical order.

Bitsight [5,6, 7]

- **Contract Vehicle:** MAS
- **SIN:** 54151ECOM
- **Contract Number:** GS35F267DA-63NLRB22F0054
- **Risk Factors Addressed:**
  - Security diligence
  - User behavior
  - Compromised systems
  - Data breaches
- **System Capabilities:**
  - Displays third-party supplier information on dashboard
  - Updates Security Ratings daily for third parties
  - Informs of any major security event and isolates suppliers that were exposed from the vulnerability
  - Streamlines outreach and communication to suppliers
  - Tracks supplier responses of remediation or mitigation efforts

Deloitte[8,9]

- **Contract Vehicles:** GWAC, MAS
- **SIN:** Multiple
- **Contract Numbers:** Multiple
- **Risk Factors Addressed:**
  - Information security
  - Cyber risk
  - Operational risk
  - Business continuity risk
  - Privacy risk
  - Performance risk
  - Regulatory compliance
- **System Capabilities:**
  - Constantly monitors third-party vendors
  - Aggregates data collected about vendors into dashboards
  - Delivers risk insights as an interactive management action plan
  - May provide services via technology platforms already used by customers

Dun and Bradstreet[10,11]

- **Contract Vehicle:** MAS
- **SIN:** 541611, 541690, 561450, OLM
- **Contract Number:** GS-00F-022DA
- **Risk Factors Addressed:**
  - Cyber risk
  - Financial, legal, and government indicators
  - Ultimate beneficial ownership
  - Geographic location

- **System Capabilities:**
  - Generates predictive scores and ratings in at least 10 different categories to understand supplier's level of cyber risk in specific areas
  - Provides insight into potential new suppliers prior to onboarding
  - Manages and reports on cybersecurity compliance systematically
  - Displays information on a customizable portfolio dashboard that undergoes frequent data updates
  - Proactively sets ongoing supplier monitoring with notifications of completed screenings and supplier viability in near real-time

Exiger[12,13]

- **Contract Vehicle:** MAS
- **SIN:** 54151ECOM, 54151HEAL, 54151S, 541990RISK, OLM
- **Contract Number:** GS-35F-0292U
- **Risk Factors Addressed:**
  - Cyber supply chain risk management
  - Foreign ownership, control, or influence (FOCI)
  - Financial health
  - Sanctions
- **System Capabilities:**
  - Generates list of nth tier suppliers
  - Provides scores pertaining to the riskiness of each supplier by risk type
  - Traces data sources which impact risk score so user can audit and defend risk assessment
  - Displays information on configurable dashboards
  - Dashboards are monitored in real-time and maintained by Exiger team members during course of subscription

Govini[14,15]

- **Contract Vehicle:** MAS
- **SIN:** 333249, 33411, 3361E, 493110RM, 511210, 518210C, 518210ERM, 532420L, 54137GEO, 54151, 54151ECOM, 54151S, 561422, 611420, 811212, ANCILLARY, OLM
- **Contract Number:** 47QSWA18D008F, NNG15SC73B-47QTCB22F0022
- **Risk Factors Addressed:**
  - Business sectors
  - Companies
  - Suppliers
  - Sources of capital, parts, and programs
  - New countries entering the supply chain
  - FOCI
- **System Capabilities:**
  - Presents reports in customizable dashboard
  - Generates supplier ecosystem map for both potential and existing vendors
  - Customizations of ecosystem map are possible to filter out irrelevant information
  - Updates data provided in products regularly to ensure accuracy of information

Interos[16,17,18]

- **Contract Vehicle:** MAS
- **SIN:** 541611, 541614SVC, OLM, 339940, 511210, 811212
- **Contract Number:** GS-00F-0014X
- **Risk Factors Addressed:**
  - Financial
  - Cyber
  - Restrictions
  - Geopolitical
  - Operations
- **System Capabilities:**
  - Displays reports on platform accessed in SaaS application or via Application Programming Interfaces (APIs)
  - Generates risk assessment for each risk factor addressed as high, medium, or low down to the nth tier
  - Constructs learning models for automated detection and response
  - Updates Knowledge Graph with both current and potential vendors with over 200 events every 20 seconds, maintained by Interos analysts

Other C-SCRM Related Technologies and Services Available on GSA Contract Vehicles

Anti-Counterfeiting

SIN 334419—Unique Identification (UID)/Radio Frequency Identification (RFID)

Anti-counterfeiting solutions are offered by multiple vendors under MAS Transportation and Logistics Services for a variety of applications. Methods such as UID/RFID help organizations protect against diverting the system or component for counterfeit replacement; the loss of confidentiality, integrity, or availability of the system or component function and data; and interrupting supply chain and logistics processes for critical components and supports practices stipulated under “asset monitoring and tracking” *–security control (PE-20) in NIST SP 800-161r1* where PE is the control family designator for Physical and Environmental Protection.

Business Information

SIN 561450—Business Information Services (BIS)

Agencies can procure subscription services such as Dunn and Bradstreet, LexisNexis, and Experian, which provide due diligence information on existing and potential suppliers of covered articles. Business due diligence supports supplier risk assessments and reviews as stipulated in the “supplier assessments and reviews" *–security control (SR-6) in NIST SP 800-53r5*.

Logistical Services/Supply and Value Chain Management

SIN 541614SVC—Supply and Value Chain Management

This category covers supply and value chain management activities, which involve all phases of the planning, acquisition, and management of logistics systems. As C-SCRM lies at the nexus of traditional supply chain risk management and traditional information security,[19] most, if not all, of these vendors could claim to have the capability to provide both C-SCRM advisory services as well as C-SCRM tools with additional C-SCRM specific capability requirements included in their SOW/PWS/SOO.

Cybersecurity Supply Chain Risk Management Advisory Services

Advisory services can support various C-SCRM functions in addition to SCRAs. For example, C-SCRM subject matter expert contractors can assist agencies with foundational, sustaining, and enhancing C-SCRM practices identified in NIST SP800-161r1 that are critical to agencies' success in managing supply chain risks.[20] These include the following:

- Developing, operationalizing, and managing a C-SCRM PMO or team
- Conducting C-SCRM relevant acquisition activities such as integrating C-SCRM requirements into RFPs and contracts with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers
- Supply chain risk information sharing activities
- Conducting enterprise-wide C-SCRM training and awareness
- Assisting with the development and implementation of capability measurement and C-SCRM metrics.

When acquiring C-SCRM advisory services, agencies should require knowledge of C-SCRM standards and practices, C-SCRM security controls, legislative and executive actions on C-SCRM, latest trends in cybersecurity supply chain threats, recent developments in C-SCRM, and expertise in training, program management, and policy analysis among others. Contractors maybe provide a variety of services to supplement agency staffing, including the following:

- Use supplier and product/service risk assessment tools
- Conduct initial vulnerability advisory report analysis
- Develop and execute C-SCRM strategic and implementation plans
- Develop enterprise level C-SCRM policies and a supplier management program
- Assist agencies with integrating C-SCRM into acquisition policies and strategies
- Assist with internal criticality analysis
- Manage and monitor components of embedded software to manage risk across the enterprise (e.g., SBOMs paired with criticality, vulnerability, threat, and exploitability to make this more automated).

Successfully supporting these tasks may require skill sets such as risk analysis, intelligence analysis (potentially with the ability to interpret foreign languages), systems engineering, operations research, mathematics, statistics, SCRM data analytics, and global market trends to name a few.

Many vendors on GSA’s GWACs provide access to systems design, software engineering, information assurance and enterprise architecture solutions (e.g. Alliant 2, 8(a) STARS III, and VETS 2). Agencies could leverage these broadly scoped GWACs by issuing specific task orders that require subject matter expertise specific to C-SCRM solutions within other IT requirements. Professional government consulting companies that offer C-SCRM advisory services should also be able to advise and aid agencies with the procurement of tools that they need for their C-SCRM activities.

MAS SIN 541611 “Professional Services" category and “Business Administrative Services” subcategory and GSA’s Alliant *2* contract vehicle provide agencies IT services and IT services based solutions including all aspects of supply chain management, from the initial sourcing phase through customer delivery. Agencies can leverage these contract solutions to support their C-SCRM activities with additional C-SCRM specific requirements included in task orders.

Best Practices for Developing Contract-Related Documents for C-SCRM Tools and Services

Government buyers should develop requirements for C-SCRM tools and professional services based on their C-SCRM needs (based on their agency and mission risk appetite and risk tolerance) and resources. These requirements could span from a few initial capabilities for agencies that are in the early stages of their C-SCRM program development to more comprehensive solutions and capabilities that meet the needs of agencies with more mature programs. Government buyers should seek commercial capabilities when appropriate that help them identify, assess, and address baseline risk factors listed in NIST SP 800-161r1, as well as provide information on compliance with federal restrictions that prohibit the use of certain suppliers and the acquisition or use of certain items, services, or materials. Several agencies have found it helpful to prioritize the implementation of the capabilities called out by the Government Accountability Office (GAO) Report (GAO-21-171) and the requirements for the desired level of program maturity detailed in the IG FISMA metrics related to C-SCRM. The GAO Report and IG FISMA metrics are both based on the foundational practices described in NIST SP 800-161r1.

Contract-related documentation (e.g., PWS, RFQ, SOW, etc.) should include appropriate requirements (based on the agency and program’s risk tolerance and appetite) on each of the desired C-SCRM tool capabilities listed below to assist government buyers with their C-SCRM activities.

1. **Supply Chain Risk Illumination**

- Mapping of key suppliers’ supply chains (tools and services that assist federal executive branch agencies with the illumination of supply chain and suppliers from design and development to the manufacturing of components and systems, from delivery to deployment and system integration of the technologies, and from sustaining and maintenance services to end of life disposal).
    - Identification/illumination of supplier relationships (upstream partners/suppliers and downstream partners/customers), especially those that are directly related to the specific product of concern.
    - Identification of logistics providers for each movement of hardware component/product, the software developers (to include open-source components), the resellers and distributors, the warehouses, the fulfillment centers, the integrators, the maintenance/support, the disposal services, and the critical infrastructure associated with each entity in the supply chain.
    - For service providers (i.e., cloud or Internet), the identification of their hardware/software/services suppliers which enable them to provide the service.

- Identification and assessment of supplier risks associated with:
    - Company Information: corporate family tree, years in business, mergers and acquisitions (M&As), contracts with foreign governments, customer base and trends, association with or previous experience by company leadership (Board or

C-suite in foreign government or military service), stability or high turnover or firings at senior leadership level, number of employees at specific locations and company-wide, investors/investments, patent sales to foreign entities, financial metrics and trends, financial reports and audits.

- Quality/Past Performance: past performance information, relevant customer ratings or complaints, recalls.
- Personnel: hiring history from a foreign country or foreign adversary's intelligence, military, law enforcement, or other security services, evidence of questionable loyalties and unethical or illicit behavior and activities.
- Geopolitical: location-based political upheaval or corruption, trade route disruptions, jurisdictional legal requirements, country or regional instability.
- FOCI:
    - Country is identified as a foreign adversary or country of special concern
    - Source or its component suppliers have headquarters, research, development, manufacturing, testing, packaging, distribution, or service facilities or other operations in a foreign country, including a country of special concern or a foreign adversary
    - Identified personal and/or professional ties between the entity being assessed—including its officers, directors or similar officials, employees, consultants, or contractors—and any foreign government
    - Implications of laws and regulations of any foreign country in which the source has headquarters, research development, manufacturing, testing, packaging, distribution, or service facilities or other operations.
    - Nature or degree of FOCI on a supplier
    - FOCI of any business entities involved in the supply chain, to include subsidiaries and subcontractors, and whether that ownership or influence is from a foreign adversary of the U.S. or designated country of concern.
    - Any indications that the supplier may be partly or wholly acquired by a foreign entity or a foreign adversary
    - Supplier domiciled in a country (without an independent judicial review) where the law mandates cooperation, to include the sharing of personally identifiable information (PII) and other sensitive information, with the country's security services
    - Indications that demonstrate a foreign interest's capability to control or influence the supplier's operations or management or that of an entity within the supply chain
    - Foreign nationals or key personnel from a foreign country involved with the design, development, manufacture, or distribution of the covered article (this type of information is not typically available publicly)
    - Supplier is domiciled in or influenced/controlled by a country that is known to conduct intellectual property theft against the U.S.
- Compliance/Legal: record of compliance with laws, regulations, contracts, or agreements, sanctions, trade controls, judgments/fines

  - Fraud, Corruption, Sanctions, and Alignment with Government Interest: civil or criminal litigation, history or current evidence of fraudulent activity, history of committing intellectual property theft, history of dealings in the sale of military goods, equipment, or technology to countries of concern
  - Environmental: energy scarcity, earthquakes, fire, adverse weather, and other natural disasters and potential other risk factors specific to the user's risk environment should also be included

2. **System requirements**

- In addition to the above supply chain risk due diligence information, the writers of the contract-related documentation should consider including requirements regarding the tool, product, or system solution used to deliver due diligence information (it should be noted that adding specific requirements without a good reason could exclude providers and solutions that may be helpful). Some of these considerations include the following:
  - Cloud-based services offering, preferably with a current Federal Risk and Authorization Management Program (FedRAMP) authorization
  - Confidence in the veracity of the sources of the data used
  - Up-to-the-minute output of data with future and historical data and full search capabilities displayed in a user interface
  - System capabilities related to the desired frequency of informational updates
  - Monitoring of supply chain/market/industrial base illuminations upon request
  - Ability to monitor unstructured web-based content
  - Ability to leverage commercial data tools and applications, effective data visualization capabilities, Natural Language Processing (NLP)/Neural Networks, or open-source development tools such as "R" and Python
  - Dependable availability and resilience of the service through operations and maintenance support, providing all necessary activities to sustain operating environments for the data pipeline, master dataset, and analytic application
  - Integration of data on private sector operations with known federal government contracting performance information in databases such as Contractor Performance Assessment Reporting System (CPARS) and Supplier Performance Risk System (SPRS)
  - Classification of public and private companies according to multiple industry classifications (e.g., Product Service Code (PSC), Unique Entry Identifier (UEI), Global Industry Classification Standard (GICS), Standard Industrial Classification (SIC), and North American Industry Classification System (NAICS) codes using software and analytics)
  - Access to premium commercial data sets to include, but not limited to, news media, public company data, private company data, patents, social media, global watch list, and non-traditional data sources, while obfuscating or anonymizing search and aggregation techniques as appropriate
  - Scalability (e.g., to meet spikes in demand, accommodate increases in utilization rate or number of concurrent users) and extensibility (e.g., able to be augmented with additional functionality)

    - In-depth data analysis completed and available via a transferrable medium/format (memorandum, presentation, report, etc.) and/or via a web-accessible dashboard, with the ability to drill down to individual entity data based on the agency's needs
    - Ability to access, aggregate, store, reuse, or retain supply chain risk information by the government
    - Capability to provide predictive analyses of ICT supply chain threats (e.g., using AI/ML)
    - Capability to anticipate future scenarios and make recommendations related to supply chain planning, sourcing, and transportation
    - Pricing considerations to ensure best value, such as being able to realize economies of scale, implementation affordability, and reasonableness and predictability of ongoing costs are key objectives for the government
        - Are there "cost line items" for your offering that can be priced out separately? For these cost line items, what is pricing based upon?
        - Are discounts available based on volume or other factors?
        - What are the licensing options and the impact of having additional users?
        - Does pricing depend on whether the information will be shared across the agency or between agencies?
- Ask the suppliers to provide any additional comments they may have concerning the government's pricing objectives

Regarding professional contractor support, requirements may include the following:

- Risk analysis
- Intelligence analysis (capable of interpreting foreign languages data)
- Systems engineering
- Operations research
- Mathematics and statistics
- SCRM data analytics and global market trends
- Technical expertise and demonstrated knowledge to interpret a diverse set of technologies across the relevant critical infrastructure sectors.

Appendix A: Key Federal Restrictions Related to C-SCRM

The information below was provided in NIST SP 800-161r1 in Appendix E, but is not a comprehensive list of all federal restrictions that prohibit the use of certain suppliers and the acquisition or use of certain items, services, or materials:

1. **The Specially Designated Nationals (SDN) and Blocked Persons List:** The Treasury Department, Office of Assets Control (OFAC), through EO 13694 and as amended by EO 13757, provided for the designation on the Specially Designated Nationals and Blocked Persons List (SDN List) of parties determined to be responsible for, complicit in, or to have engaged in, directly or indirectly, malicious cyber-enabled activities. Any entity in which one or more blocked persons directly or indirectly holds a 50% or greater ownership interest in the aggregate is itself considered blocked by operation of law. U.S. persons may not engage in any dealings, directly or indirectly, with blocked persons.
2. **The Sectoral Sanctions Identifications (SSI) List:** The sectoral sanctions imposed on specified persons operating in sectors of the Russian economy identified by the Secretary of the Treasury were done under EO 13662 through Directives issued by OFAC pursuant to its delegated authorities. The SSI List identifies individuals who operate in the sectors of the Russian economy with whom U.S. persons are prohibited from transacting with, providing financing for, or dealing in debt with a maturity of longer 90 days.
3. **The Foreign Sanctions Evaders (FSE) List:** OFAC publishes a list of foreign individuals and entities determined to have violated, attempted to violate, conspired to violate, or caused a violation of U.S. sanctions on Syria or Iran pursuant to EO 13608. It also lists foreign persons who have facilitated deceptive transactions for or on behalf of persons subject to U.S. sanctions. Collectively, such individuals and companies are called "Foreign Sanctions Evaders" or "FSEs." Transactions by U.S. persons or within the U.S. involving FSEs are prohibited.
4. **The System for Award Management (SAM) Exclusions:** The SAM contains the electronic roster of debarred companies excluded from federal procurement and nonprocurement programs throughout the U.S. Government (unless otherwise noted) and from receiving federal contracts or certain subcontracts and from certain types of federal financial and non-financial assistance and benefits. The SAM system combines data from the Central Contractor Registration, Federal Register, Online Representations and Certification Applications, and the Excluded Parties List System. It also reflects data from the Office of the Inspector General's exclusion list (GSA) (CFR Title 2, Part 180).
5. **The List of Foreign Financial Institutions Subject to Correspondent Account Payable-Through Account Sanctions (the "CAPTA List"):** The CAPTA List replaced the list of Foreign Financial Institutions Subject to Part 561. It includes the names of foreign financial institutions subject to sanctions, certain prohibitions, or strict conditions before a U.S. company may do business with them.
6. **The Persons Identified as Blocked:** Pursuant to 31 CFR 560 and 31 CFR 560.304, property and persons included on this list must be blocked if they are in or come within the possession or control of a U.S. person.
7. **The BIS Unverified List:** Parties listed on the Unverified List (UVL) are ineligible to receive items subject to the Export Administration Regulations (EAR) by means of a license exception.

8. **The 2019 National Defense Authorization Act, Section 889:** Unless a waiver or exception is granted, NDAA Section 889 prohibits the federal government, government contractors, and grant and loan recipients from procuring or *using* certain "covered telecommunication equipment or services" that are produced by Huawei, ZTE, Hytera, Hikvision, Dahua, and their subsidiaries as a "substantial or essential component of any system or as critical technology as part of any system."
9. Any other federal restriction or law that would restrict the acquisition of goods, services, or materials from a supplier.

Appendix B: Inherited Third-Party Risks

The table below was taken from NIST SP 800-161r1 and is representative of the types of risk categories and factors that should be considered when conducting risk assessments. It should be noted that some of the factors are not readily available through publicly available information, so the Supply Chain Risk Illumination tools being leveraged may not be able to provide a comprehensive view of the risks associated with a particular supplier or their supply chain. Additional categorizations and lists of risk factors have been published by other agencies, public-private partnerships, and industry associations and may be consulted for potential inclusion in each agency's C-SCRM program as applicable.

Baseline Risk Factor	Definition or Guidance	Non-exclusive Indicators of Risk (as applicable)
Functionality, features, and components of the covered article	Information informs a determination as to whether the product or service is "fit for purpose" and the extent to which there is assurance that the applicable C-SCRM dimensions (see Section 1.4 of main body) are satisfied, and/or there are inherent or unmitigated weaknesses or vulnerabilities.	• Ability of the source to produce and deliver the product or service as expected • Built-in security features and capabilities or lack thereof • Who manages or has ultimate control over security features • Secure configuration options and constraints • Management and control of security features (who, how) • Network/internet connectivity capability or requirements and methods of connection • Software and/or hardware bill of materials • Any transmission of information or data (to include, if known, the identification of the source and location of the initiator or recipient of the transmission) to or by a covered article necessary for its function
Company (i.e., source) Information	Information about the company, to include size, structure, key leadership, and financial health.	• Corporate family tree • Years in business • Merger and acquisition activity (past and present) • Contracts with foreign governments • Customer base and trends • Association or previous experience by company leadership (Board or C-suite in foreign government or military service) • Stability or high turnover or firings at senior leadership level • Number of employees at specific location and company-wide • Investors/investments • Patent sales to foreign entities

		• Financial metrics and trends • Financial reports/audits
Quality/Past Performance	Information about the ability of the source to produce and deliver covered articles as expected. This includes an understanding of the quality assurance practices associated with preventing mistakes or defects in manufactured/developed products and avoiding problems when delivering solutions or services to customers.	• Past performance information • Relevant customer ratings or complaints • Recalls • Quality metrics Evidence of a quality program and/or certification
Personnel	Information about personnel affiliated with or employed by the source or an entity within the supply chain of the product or service.	• The supplier's program to vet its personnel, to include whether there is an insider threat program, and/or whether the supplier performs background checks and prior employment verification • Hiring history from a foreign country or foreign adversary's intelligence, military, law enforcement or other security services • Turnover rate • Staffing level and competencies • Evidence of questionable loyalties and unethical or illicit behavior and activities
Physical	Information associated with the physical aspects of the environment, structures, facilities, or other assets sufficient to understand if/how they are secured and the consequences if damaged, unavailable, or compromised.	• Evidence of the effectiveness of physical security controls, such as procedures and practices that ensure or assist in the support of physical security • Proximity to critical infrastructure or sensitive government assets or mission functions • Natural disasters or seismic and climate concerns
Geopolitical	Information associated with a geographic location or region of relevance to the source or the supply chain associated with the source, product, and/or service.	• Location-based political upheaval or corruption • Trade route disruptions • Jurisdictional legal requirements • Country or regional instability
Foreign Ownership, Control, or	Ownership of, control of, or influence over the source or covered article(s) by a	• Country is identified as a foreign adversary or country of special concern

Influence (FOCI)	foreign interest (e.g., foreign government or parties owned or controlled by a foreign government, or other ties between the source and a foreign government) has the power, direct or indirect, whether or not exercised, to direct or decide matters that affect the management or operations of the company.	• Source or its component suppliers have headquarters, research, development, manufacturing, testing, packaging, distribution, or service facilities or other operations in a foreign country, including a country of special concern or a foreign adversary • Identified personal and/or professional ties between the source—including its officers, directors or similar officials, employees, consultants, or contractors— and any foreign government • Implications of laws and regulations of any foreign country in which the source has headquarters, research development, manufacturing, testing, packaging, distribution, or service facilities or other operations • Nature or degree of FOCI on a supplier • FOCI of any business entities involved in the supply chain, to include subsidiaries and subcontractors, and whether that ownership or influence is from a foreign adversary of the United States or country of concern • Any indications that the supplier may be partly or wholly acquired by a foreign entity or a foreign adversary • Supplier domiciled in a country (without an independent judicial review) where the law mandates cooperation, to include the sharing of PII and other sensitive information, with the country's security services • Indications that demonstrate a foreign interest's capability to control or influence the supplier's operations or management or that of an entity within the supply chain • Key management personnel in the supply chain with foreign influence from or with a connection to a foreign government official or entities, such as members of the board of directors, officers, general partners, and senior management official • Foreign nationals or key management personnel from a foreign country involved with the design, development, manufacture or distribution of the covered article

		• Supplier's known connections to a foreign country or foreign adversary's intelligence, law enforcement, or other security service • Supplier is domiciled in or influenced/controlled by a country that is known to conduct intellectual property theft against the U.S.
Compliance/Legal	Information about noncompliance, litigation, criminal acts, or other relevant legal requirements.	• Record of compliance with pertinent U.S. laws, regulations, contracts, or agreements • Sanctions compliance • Trade controls compliance • Judgments/Fines
Fraud, Corruption, Sanctions, and Alignment with Government Interests	Information about past or present fraudulent activity or corruption and being subject to suspension, debarment, exclusion, or sanctions (also see Table E-2 in NIST SP 800-161r1 and discussion immediately preceding table).	• Civil or criminal litigation • Past history or current evidence of fraudulent activity • Source's history of committing intellectual property theft • Supplier's dealings in the sale of military goods, equipment, or technology to countries that support terrorism or proliferate missile technology or chemical or biological weapons and transactions identified by the Secretary of Defense as "posing a regional military threat" to the interests of the U.S. • Source's history regarding unauthorized technology transfers
Cybersecurity	Information about the cybersecurity practices, vulnerabilities, or incidents of the source, product, service, and/or supply chain.	• Evidence of effective cybersecurity policies and practices • Supplier's history as a victim of computer network intrusions • Supplier's history as a victim of intellectual property theft • Information about whether a foreign intelligence entity unlawfully collected or attempted to acquire an acquisition item, technology, or intellectual property • Existence of unmitigated cybersecurity vulnerabilities • Indication of malicious activity—including subversion, exploitation, or sabotage—associated with the supplier or the covered article • Any unauthorized transmission of information or data by a covered article to a country outside of the U.S.
Counterfeit and Non-Conforming Products (include in	Information about counterfeits, suspected	• Evidence or history of counterfeits or non-conforming products associated with the supplier

baseline if relevant to source and/or product being assessed; if in doubt, include)	counterfeits, gray market, or non-conforming products.	• Suppliers' anti-counterfeit practices and controls • Sourcing of components from the gray market
Supply Chain Relationships, Visibility, and Controls	Information about the supply chain associated with the source and/or covered article.	• Evidence of effective C-SCRM and supplier relationship management practices • Components or materials (relevant to covered article) originate from single source in upstream supply chain • Reliance on single trade route • Provenance of the product

Appendix C: Supplemental Information on Select Supply Chain Risk Illumination Tools Available on GSA Contract Vehicles

Company: Bitsight

Bitsight is a cloud-based cyber risk management SaaS provider. Two of Bitsight's main products are the Bitsight Security Rating and Third-Party Vulnerability Response platform. These products have been developed to help businesses make informed risk management decisions and strengthen their overall security posture.

Bitsight's Security Rating is a numerical metric which can be linked to the likelihood of a cyber breach and the performance of an organization's cybersecurity program over time. Bitsight describes its Security Rating akin to a credit score. The Security Rating of an organization can be classified into three categories: Basic (250 – 630), Intermediate (630 – 740), and Advanced (740+).[21] These Security Ratings can be coupled with Bitsight's Third-Party Vulnerability Response platform to provide findings related to the following risk factors:[22]

- Security diligence
- User behavior
- Compromised systems
- Data breaches.

There are a total of 23 different risk vectors evaluated using Bitsight's products and the findings of each risk vector are broken into five categories—good, fair, neutral, warn, or bad. These rankings correlate to cumulative grades of A-F.[23] The data collection process to generate a finding for each risk vector leverages both human and machine intelligence. When mapping a network, both public data and patented methods are employed to understand an organization's assets.[24]

The information found pertaining to third-party suppliers is displayed as a dashboard. Depending on the subscription agreement, different features can be accessed regarding suppliers through the dashboard. For example, in the Total Risk Monitoring subscription, users have access to fourth party visibility and the risk vector grades for each of their critical third parties, but do not have access to these pieces of information in the Risk Monitoring subscription. It should be noted that users can switch between subscription types during their contract with Bitsight.[25]

The Third-Party Vulnerability Response dashboard highlights, in close to real-time, any major security event and which vendors in the supply chain are exposed from the vulnerability.[26] From the dashboard, outreach can be initiated to any or all exposed vendors to speed along remediation or mitigation efforts from exposed vendors. Additionally, users can track vendor responses to know which vendors have received, completed, or remediated the vulnerability to inform your next steps as an organization to protect against the vulnerability.[27]

Company: Deloitte

Deloitte is a global provider of audit and assurance, consulting, financial advisory, tax, and other related services. Deloitte offers services to organizations in both the federal and commercial sectors. One service Deloitte offers is third-party risk management (TPRM) solutions and since 2007, Deloitte has offered a proprietary supply chain analytics tool, known as CentralSight.[28]

Deloitte's CentralSight is designed to illuminate supply chains and inform supply chain risk management decisions. It is an AI-powered software and ML-enabled entity resolution platform. Deloitte's CentralSight and TPRM services can be purchased as subscription services. These products allow users to visualize and make informed decisions regarding the entirety of their supplier ecosystem by using four steps: illuminate, triage, mitigate, and monitor.[29] Through these four steps, Deloitte's products can provide the following:

- Visualization of global networks up to 12th tier
- Identification of suppliers in the network that are most critical to a healthy supplier ecosystem using network analysis theory and 24 risk lenses
- Creation of actionable insights for risk mitigations based on suppliers that pose risk to brand, reputation, revenue, profitability, national defense, or public health
- Observation and monitoring of supplier ecosystems

Some risk factors that Deloitte's products can report on the following:[30]

- Information security
- Cyber risk
- Operational risk
- Business continuity risk
- Privacy risk
- Performance risk
- Regulatory compliance.

Deloitte offers constant monitoring of third-party vendors. The TPRM platform can aggregate data from assessments to generate dashboards and other reporting components to display a vendor's risk to the supply chain.[31] Deloitte provides risk awareness and business insights by aggregating data from internal data sets and intellectual property (e.g., risk taxonomy, key performance indicators (KPI) library, and prebuilt maturity models), as well as more than 1,200 third-party data sources.[32] Their proprietary platforms combine mobile data-collection, performance improvement tools, and mobile optimized dashboards to deliver risk management insights to customers. Deloitte may also be able to provide services to customers using technology platforms already used by their organization.[33]

Company: Dun and Bradstreet

Dun and Bradstreet (D&B) is a Business-to-Business (B2B) provider of commercial data, analytics, and insights. Its global database houses information on more than 500 million companies and D&B uses this database to provide awareness about their customers' suppliers. Their main product pertaining to supply chain risk management is a platform known as D&B Risk Analytics–Supplier Intelligence.[34]

D&B Risk Analytics–Supplier Intelligence, an AI-powered solution, is designed to anticipate and mitigate supplier risk. D&B Risk Analytics–Supplier Intelligence is a subscription-based software[35] which leverages data from D&B Data Cloud to screen and monitor supplier risk.[36] The key components of D&B Risk Analytics–Supplier Intelligence include monitoring and alerts, locating different suppliers, sanctions screening, and reporting and analysis. Through D&B's products, customers could receive notifications about suppliers' vulnerabilities prior to disrupting the supply chain, and identify alternative suppliers filtered by industry, location, size, and risk scores. Customers can also choose to conduct a quick or more thorough restrictive party screening using Dow Jones' global database and assess their portfolio using various risk factors. When assessing their supplier portfolio, customers will be provided D&B's proprietary predictive risk scores and ratings. These predictive risk scores and ratings include assessments of suppliers':[37]

- Cyber risk
- Financial, legal, and government indicators
- Ultimate beneficial ownership
- Geographic location.

D&B products can generate predictive scores and ratings in at least seven distinct categories, including one titled D&B Risk Rankings. This ranking is powered by SecurityScorecard and offers insight into a supplier's cybersecurity performance. A supplier's ranking is divided into ten separate categories to help customers understand their supplier's level of cyber risk in specific areas. Some feature highlights of the D&B Risk Rankings include getting insight about potential new suppliers prior to onboarding them, understanding current suppliers' cybersecurity strengths, and systematically managing and reporting on cybersecurity compliance.[38]

Information generated by D&B Risk Analytics–Supplier Intelligence is displayed to customers using a portfolio dashboard. This user interface is customizable and undergoes frequent data updates. Customers can also set ongoing supplier monitoring with notifications of completed screenings and supplier viability to proactively understand their supply chain in near real-time.[39]

Company: Exiger

Exiger is a global risk and compliance SaaS company that provides a range of services to help organizations manage risk and ensure compliance with legal and regulatory requirements. Exiger has developed a proprietary framework called TRADES (Transparency of current state, Risk methodology design, Assess current risks, Determine mitigations, Evaluate framework uplift, Supplier monitoring) that enables organizations to enhance their supply chain resilience and improve their risk management capabilities regardless of their level of maturity in these areas.[40] Two of the main products offered by Exiger include Due Diligence IQ (DDIQ) and Supply Chain Explorer.

DDIQ is an AI-powered research engine designed for users to automate and streamline their due diligence and compliance processes by leveraging artificial intelligence. Supply Chain Explorer is a SaaS analytics application which provides single-click supply chain risk detection.[41] Both DDIQ and Supply Chain Explorer are subscription-based services. All DDIQ subscriptions include access to the DDIQ Analytics Platform and Standard Dashboards. It should be noted that significant customization of the dashboards and/or requesting data sources not already included in DDIQ is possible but could be priced separately.[42]

Reports produced using Exiger's products could include evaluations related to:[43]

- Cyber supply chain risk management (C-SCRM)
- FOCI
- Financial health
- Financial crime compliance
- Sanctions
- The target entity's list of n^{th} tier suppliers
- Scores pertaining to the riskiness of each supplier by risk type
- Tracing the data sources which impact the risk score so that the user can fully audit and defend the risk assessment.

Reports provided by Exiger are generated by aggregating data from internal and external open data sets, which include, but are not limited to, direct unstructured and structured data sources, contract records, source records of supply chain installations, and unique supply chains.[44] Results generated are continuously monitored in real time (as source data is updated) and can be viewed on configurable dashboards. These dashboards are maintained by Exiger team members throughout the course of the subscription.[45]

Exiger uses RiskIQ, which is an automated risk rating product. RiskIQ sources over 300 data points on every third party listed in the DDIQ report. These data points contribute to a risk assessment score. Through these risk assessment scores, vendors can be classified according to low, medium, and high risk.[46] Categorizing using these classifications helps users see which vendors pose the most significant risk to an organization.

Company: Govini

Govini is a business intelligence platform which uses commercial data to provide services for companies and agencies across the federal market. Govini's primary products include the Decision Science Platform, National Security Knowledge Graph, and Ark.ai.

Govini's Decision Science Platform and National Security Knowledge Graph are designed to help provide customers with many avenues to make informed decisions related to their industry. The Decision Science Platform can provide companies and agencies with insights pertaining to their supply chain and logistics, resourcing and reform, technology and innovation, and defense industrial base.[47] The National Security Knowledge Graph displays all available market data about government activities and related private sector research, and technology. This graph can be accessed either through the Decision Science Platform or as a direct data feed.[48] Another of Govini's products is Ark.ai, a subscription-based Commercial Data platform which has been configured for National Security.[49]

Govini's products can leverage AI/ML to tackle problems related to acquisition, foreign influence and adversarial capital, nuclear modernization, procurement, science and technology, and supply chain.[50] When evaluating a supply chain, Govini's products allow customers to examine various configurable risk factors including the following:[51]

- Business sectors
- Companies
- Suppliers
- Sources of capital, parts, and programs
- New countries entering the supply chain
- FOCI.

The reports generated by Ark.ai are presented to users in a dashboard. This dashboard portfolio is customizable and allows users to filter out irrelevant information to their search. For example, when looking for potential new vendors to add to a supply chain, an ecosystem map of the potential vendor's supply chain can be analyzed. This map can display the supplier, customer, shipper, shipping consignee, prime contractor, and sub-contractor for this vendor. Other filter criteria could include vendor's locations, foreign entities,, ownership, foreign partnerships and subsidiaries, and legal and financial information about the potential vendor.[52] The data provided in Ark.ai is updated regularly to ensure accuracy of information.

Company: Interos

Interos is a SaaS company with a focus on operational resilience and supply chain risk management. The SaaS platform is AI-powered and provides maps and models of a live global view of an organization's ecosystem.[53]

Some of the main products offered by Interos include its Business Relationship Intelligence Platform, Knowledge Graph, and i-Score^{TM}. The Business Relationship Intelligence Platform aims to increase visibility and perform a multi-factor assessment of an organization's risk beyond its third-party vendors. The Interos Knowledge Graph can be displayed with both current and potential new vendors and is updated with over 200 events every 20 seconds. This graph is monitored and maintained by Interos analysts to ensure data is accurate and precise.[54]

The i-Score^{TM} is a scale used to measure the health of an organization's supply chain and the global ecosystem in which they operate. The model used to update an organization's i-Score^{TM} can detect potential cyber activity that would be harmful to the supply chain—regardless of public disclosure. The i-Score^{TM} is a combination of commercial cyber ratings, vulnerability information (CVEs), threat assessments (MITRE ATT&CK), cyber events, regulatory compliance, and operating country into a single score. This score can be updated based on new information available.[55]

Interos maintains an operational resilience cloud which maps, monitors, and generates models of supply chains and business relationships.[56] Using Interos products, the health of a supply chain can be examined against six risk factors:[57]

- Financial
- Cyber
- Restrictions
- Geopolitical
- Operations

After examining each of the six risk factors, reports can be generated that indicate if an organization's risk in each area is high, medium, or low down to the nth tier. Reports provided by Interos are produced by using at least 85,000 aggregated data sources. The compiled data sources, combined with machine learning, construct learning models for automated detection and response. The platform which displays these reports can be accessed in a SaaS application or via APIs.[58]

Appendix D: Sources and Resources

Executive Orders:

- Executive Order 13873, *Securing the Information and Communications Technology and Services Supply Chain* (May 15, 2019)
- Executive Order 14017, *Executive Order on America's Supply Chains* (February 24, 2021)
- Executive Order 14028, *Executive Order on Improving the Nation's Cybersecurity* (May 12, 2021)
- Executive Order 14034, *Executive Order on Protecting Americans' Sensitive Data from Foreign Adversaries* (June 9, 2021)

Legislation, Regulations, and Directives:

- SECURE Technology Act – *Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act*, Public Law 115-390
- FITARA – *Federal Information Technology Acquisition Reform Act*
- FISMA – *Federal Information Security Modernization Act* of 2014 (Pub. L. No. 113-283, December 18, 2014)
- FASCSA – *Federal Acquisition Supply Chain Security Act* of 2018
- FASCSA Interim Final Rule (September 1, 2020)
- Section 889 of the 2019 National Defense Authorization Act - *Prohibition on Certain Telecommunications and Video Surveillance Services or Equipment*
- Committee on National Security Systems (CNSSD) No. 505 *Supply Chain Risk Management (SCRM)*
- OMB Circular A-130 *Managing Information as a Strategic Resource* (July 28, 2016)
- OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control* (as revised via OMB M-16-17 on July 15, 2016)
- OMB M-15-14 *Management and Oversight of Federal Information Technology* (June 10, 2015)
- OMB M-22-18 *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices* (September 14, 2022)
- OMB M-23-16 *Update to Memorandum M-22-18* (June 9, 2023)
- GAO-14-704G *Standards for Internal Control in the Federal Government* (September 2014)
- Securing the Information and Communications Technology and Services Supply Chain Interim Final Rule (15 CFR Part 7, Regulation Identifier Number (RIN) 0605–AA51, January 19, 2021)
- Federal Acquisition Regulation (FAR)
- Federal Acquisition Regulation (FAR), Part 4 *Administrative and Information Matters*
- Federal Acquisition Regulation (FAR), Part 7 *Acquisition Planning*
- Defense Federal Acquisition Regulation Supplement (DFARS)
- NASA Federal Acquisition Regulation Supplement (NFS)

Guidelines and Standards:

- NIST Framework for Improving Critical Infrastructure Cybersecurity (February 12, 2014)
- NIST Cybersecurity Framework V1.1(April 2018)
- NIST SP 800-37r2 *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* (December 2018)
- NIST SP 800-39 *Managing Information Security Risk: Organization, Mission, and Information System View* (March 2011)
- NIST SP 800-53r5 *Security and Privacy Controls for Federal Information Systems and Organizations* (September 2020)
- NIST SP 800-63B *Digital Identity Guidelines, Authentication and Lifecycle Management* (June 2017)
- NIST SP 800-161r1 *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations* (May 2022)
- NIST SP 800-171r2 *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* (February 2020)
- NIST SP 800-207 *Zero Trust Architecture* (August 2020)
- NIST SP 800-218 *Secure Software Development Framework* (February 2022)
- NISTIR 7622 *Notional Supply Chain Risk Management Practices for Federal Information Systems* (October 2012)
- NISTIR 8276 *Key Practices in Cyber Supply Chain Risk Management* (February 2021)
- International Standards Organization (ISO) 20243 *Mitigating Maliciously Tainted and Counterfeit Products* (February 2018)
- ISO 27036 *Information Security for Supplier Relationships* (2016-2023)

Additional Resources:

- GAO-21-171 *Information and Communications Technology: Federal Agencies Need to Take. Urgent Action to Manage Supply Chain Risks* (December 2020)
- Office of the Director of National Intelligence (ODNI) Supply Chain Risk Management Best Practices and ODNI Baker's Dozen
- Government Industry Data Exchange Program (GIDEP)
- National Counterintelligence and Security Center (NCSC) 2018 Foreign Economic Espionage in Cyberspace Report
- *FACT SHEET: Biden-Harris Administration Announces National Cybersecurity Strategy*
- GSA FAS ICT Acquisition Guide Training Materials (Available only to members of the government-only GSA C-SCRM Acquisition Community of Practice (ACoP))
- Federal Acquisition Certification (FAC)-093 *Introduction to Supply Chain Risk Management*
- Information Technology Sector Baseline Risk Assessment, Department of Homeland Security, August 2009.
- GSA Best in Class IT Hardware and Software
- GSA Cybersecurity Supply Chain Risk Management Guide (August 2022)

Appendix E: Acronyms

ACoP – Acquisition Community of Practice

AI – Artificial Intelligence

API – Application Programming Interface

BIS – Business Information Services

B2B – Business to Business

CAPTA – Correspondent Account Payable Through Account Sanctions

CDM – Continuous Diagnostics and Mitigation

CFR – *Code of Federal Regulations*

CNSSD – Committee on National Security Systems

CO – Contracting Officer

COR – Contracting Officer Representative

COTS – Commercial off-the-shelf

COVID-19 – Coronavirus Disease 2019

CPARS – Contractor Performance Assessment Reporting System

C-SCRM – Cybersecurity Supply Chain Risk Management or Cyber Supply Chain Risk Management

CVE – Common Vulnerability Exposure

DDIQ – Due Diligence IQ

DFARS – *Defense Federal Acquisition Regulation Supplement*

D&B – Dun and Bradstreet

EAR – Export Administrative Regulations

EO – Executive Order

FAC – Federal Acquisition Certification

FAR – *Federal Acquisition Regulation*

FAS – Federal Acquisition Service

FASC – Federal Acquisition Security Council

FASCSA – *Federal Acquisition Supply Chain Security Act of 2018*

FedRAMP – *Federal Risk and Authorization Management Program*

FISMA – *Federal Information Security Modernization Act*
FITARA – *Federal Information Technology Acquisition Reform Act*

FOCI – Foreign Ownership, Control, or Influence

FSE – Foreign Sanctions Evaders

GAO – Government Accountability Office

GICS – Global Industry Classification Standard

GIDEP – Government-Industry Data Exchange Program

GSA – General Services Administration

GWAC – Governmentwide Acquisition Contract

HACS – Highly Adaptive Cybersecurity Services

HBOM – Hardware Bill of Materials

ICAM – Identity, Control, and Access Management

ICT – Information and Communication Technologies, also referred to as Information and Communication Technologies and Services (ICTS)

IG – Inspector General

IPS – Identity Protection Services

IoT – Internet of Things

ISO – International Standards Organization

IT – Information Technology

ITC – Information Technology Category

KEV – Known Exploited Vulnerability

KPI – Key Performance Indicators

MAS – Multiple Award Schedule

ML – Machine Learning

M&A – Mergers and Acquisitions

MPC – MetaPhase Consulting

NAICS – North American Industry Classification System

NASA – National Aeronautical and Space Administration

NCSC – National Counterintelligence and Security Center

NDAA – *National Defense Authorization Act*

NFS – *NASA FAR Supplement*

NIST – National Institute of Standards and Technology
NISTIR - National Institute of Standards and Technology Interagency or Internal Report

NLP – Natural Language Processing

NSS – National Security Systems

ODNI – Office of the Director of National Intelligence

OFAC – Office of Assets Control

OMB – Office of Management and Budget

OT – Operational Technology

PE – Physical and Environmental Protection

PII – Personally Identifiable Information

PMO – Program Management Office

PSC – Product Service Code

PWS – Performance Work Statement(s)

RA – Risk Assessment

RFI – Request(s) for Information

RFID – Radio Frequency Identification

RFP – Request for Proposal

RFQ – Request for Quote

RIN – Regulation Identifier Number

SaaS – Software as a Service

SAM – System for Award Management

SBOM – Software Bill of Materials

SCRA – Supply Chain Risk Assessment

SCRM – Supply Chain Risk Management

SDLC – Secure development life cycle

SDN – Specially Designated Nationals

SECURE – *Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure*

SIC – Standard Industrial Classification

SIN – Special Item Number

SOO – Statement(s) of Objective

SOW – Statement(s) of Work

SP – Special Publication
SPRS – Supplier Performance Risk System

SR – Supply Chain Risk

SSDF – Secure Software Development Framework

SSI – Sectoral Sanctions Identifications

SSN – Sources Sought Notice(s)

STARS – Streamlined Technology Acquisition Resource for Services

TPRM – Third-Party Risk Management

TRADES – Transparency of current state, Risk methodology design, Assess current risks, Determine mitigations, Evaluate framework uplift, and Supplier monitoring

UEI – Unique Entity Identifier

UID – Unique Identification

U.S. – United States

USC – *United States Code*

UVL – Unverified List

VETS – Veterans Technology Services

ZTE – Zhongxing Telecommunications Equipment Corporation

Note: All links in the document were accessed on July 14, 2023 unless otherwise noted.

[1] According to the FASCSA the term "covered articles" means: "information technology, including cloud computing services of all types, telecommunications equipment or telecommunications service, the processing of information on a Federal or non-Federal information system, subject to the requirements of the Controlled Unclassified Information program; or hardware, systems, devices, software, or services that include embedded or incidental information technology."

[2] Department of Homeland Security, Information Technology Sector Baseline Risk Assessment, August 2009.

[3] "Open FAR Cases as of 6/16/2023." Accessed June 16, 2023. https://www.acq.osd.mil/dpap/dars/opencases/farcasenum/far.pdf.

[4] The HACS SIN is part of the Multiple Award Schedule (MAS) Information Technology and is designed to provide government organizations with access to qualified cybersecurity vendors and to help organizations meet IT security requirements. HACS ordering guide can be found at: https://www.gsa.gov/technology/technology-products-services/it-security/highly-adaptive-cybersecurityservices-hacs.

[5] "Improving Security Posture with Cyber Risk Ratings." *Cyber Risk Rating | Bitsight*, www.bitsight.com/glossary/cyber-risk-rating.

[6] "Bitsight for Supply Chain Cybersecurity Risk Management." *Supply Chain Cybersecurity Risk Management*, https://www.bitsight.com/uses/supply-chain-cybersecurity-risk-management.

[7] "Introducing Bitsight Third-Party Vulnerability Response." Performance by Jacob Mulberry, *YouTube*, YouTube, April 20, 2023. https://www.youtube.com/watch?v=YNTf5_QRI3I.

[8] "Third Party Risk Management - Handout." December 8, 2020. https://www2.deloitte.com/content/dam/Deloitte/dk/Documents/risk/TPRM%20Handout.pdf.

[9] "Third Party Risk Management: Managed Service: Deloitte Global." *Deloitte*, www.deloitte.com/global/en/services/risk-advisory/services/third-party-risk-management.html. Accessed May 15, 2023.

[10] Dun and Bradstreet. *D&B Analytics Supplier Intelligence*. https://www.dnb.com/products/third-partyrisk/dnb-risk-analytics.html

[11] "D&B Risk Analytics - Supplier Intelligence." *YouTube*, YouTube, 12 July 2022. https://www.youtube.com/watch?v=2yjrYzAo1B4.

[12] *Exiger Selected as Government-Wide Enterprise Supply Chain and Third-Party Risk Management Platform*, August 4, 2022. https://www.carrickcapitalpartners.com/exiger-selected-as-government-wideenterprise-supply-chain-and-third-party-risk-management-platform.

[13] "MAS ITC Contract Number: GS-35F-0292U." https://www.gsaadvantage.gov/ref_text/GS35F0292U/0XY2JF.3TOFE6_GS-35F0292U_CSIEGSFSSPRICELISTPA57.PDF.

[14] "Supply Chain & Logistics." *Govini*, January 15, 2023. https://govini.com/applications/supply-chainlogistics/.

[15] "Ark.Ai - Find America's Edge." *Ark.Ai - Find America's Edge*, https://ark.ai/.

[16] "Supply Chain Risk Management Technology." *Interos*, www.interos.ai/why-interos/, Accessed February 6, 2023.

[17] "Product Overview - Interos." *YouTube*, YouTube, August 12, 2021. https://www.youtube.com/watch?v=D74sT70vHtA&t=1s.

[18] "Commercial Data Sheet - November 2019." Interos, November 2019.

[19] NIST SP 800-161r1, page 1–2.

[20] NIST SP 800-161r1 identifies three categories of C-SCRM capabilities: foundational, sustaining and enhancing.

[21] "What Is a BitSight Security Rating?" *BitSight Security Rating*, https://service.bitsighttech.com/trust/landing/generic.html.

[22] "Improving Security Posture with Cyber Risk Ratings." *Cyber Risk Rating | Bitsight*, www.bitsight.com/glossary/cyber-risk-rating.

[23] Poulin, Chris. "Practitioner's Corner: Reading the Tea Leaves: Interpreting the Bitsight Rating and Risk Vectors." *Bitsight*, 20 Feb. 2023. www.bitsight.com/blog/practitioners-corner-reading-tea-leavesinterpreting-bitsight-rating-and-risk-vectors.

[24] "What Is a BitSight Rating and Why Should You Consider Using It to Manage Cyber Risk in Your Supply Chain." *What Is a BitSight Rating and Why Should You Consider Using It*, https://www.epiqglobal.com/en-us/resource-center/articles/what-is-a-bitsight-rating.

[25] "BitSight TPRM Subscriptions Explained." Bitsight. https://www.bitsight.com/sites/default/files/202210/TPRM%20Subscriptions%20Comparison%20Data%20Sheet.pdf.

[26] "Bitsight for Supply Chain Cybersecurity Risk Management." *Supply Chain Cybersecurity Risk Management*, https://www.bitsight.com/uses/supply-chain-cybersecurity-risk-management.

[27] "Introducing Bitsight Third-Party Vulnerability Response." Performance by Jacob Mulberry, *YouTube*, YouTube, April 20, 2023. https://www.youtube.com/watch?v=YNTf5_QRI3I.

[28] "CentralsightTM: Supply Chain Analytics Tool." *Deloitte United States,* https://www2.deloitte.com/us/en/pages/public-sector/solutions/central-sight-supply-chain-analytics.html.

[29] "Supply Chain in Government: Enhancing Supplier Networks to Ensure Performance, Resilience, and Security." https://www2.deloitte.com/content/dam/Deloitte/us/Documents/public-sector/us-enhancing-supplier-networks.pdf.

[30] "Third Party Risk Management - Handout." December 8, 2020. https://www2.deloitte.com/content/dam/Deloitte/dk/Documents/risk/TPRM%20Handout.pdf.

[31] "Third Party Risk Management - Handout." December 8, 2020. https://www2.deloitte.com/content/dam/Deloitte/dk/Documents/risk/TPRM%20Handout.pdf.

[32] "Supplier Risk Management." *Supplier Risk Management | Deloitte US*, https://www2.deloitte.com/us/en/pages/operations/solutions/supplier-risk-management.html.

[33] "Third Party Risk Management: Managed Service: Deloitte Global." *Deloitte*, www.deloitte.com/global/en/services/risk-advisory/services/third-party-risk-management.html. Accessed May 15, 2023.

[34] "Try D&B Risk Analytics - Supplier Intelligence Free." *Try D&B Risk Analytics Free*, https://www.dnb.com/marketing/media/dnb-risk-analytics-free-trial.html.

[35] "Third-Party Risk Tools." *Third-Party Risk Products - Risk, Spending & Onboarding Tools*, https://www.dnb.com/products/third-party-risk.html.

[36] "D&B Risk Analytics - Supplier Intelligence." *YouTube*, YouTube, 12 July 2022. https://www.youtube.com/watch?v=2yjrYzAo1B4.

[37] Dun and Bradstreet. *D&B Analytics Supplier Intelligence*. https://www.dnb.com/products/third-partyrisk/dnb-risk-analytics.html

[38] Dun and Bradstreet. *D&B Analytics Supplier Intelligence*. https://www.dnb.com/products/third-partyrisk/dnb-risk-analytics.html

[39] "D&B Risk Analytics - Supplier Intelligence." *YouTube*, YouTube, 12 July 2022. https://www.youtube.com/watch?v=2yjrYzAo1B4.

[40] "Introducing: TRADES." *Third Party and Supply Chain Risk Management Framework*, https://resources.exiger.com/risk-management-in-supply-chain.

[41] "Exiger Launches First Ever Single-Click Supply Chain Risk Detection SaaS Platform." *Exiger*, March 31, 2022. www.exiger.com/perspectives/exiger-launches-supply-chain-explorer/.

[42] "MAS ITC Contract Number: GS-35F-0292U." https://www.gsaadvantage.gov/ref_text/GS35F0292U/0XY2JF.3TOFE6_GS-35F0292U_CSIEGSFSSPRICELISTPA57.PDF.

[43] *Exiger Selected as Government-Wide Enterprise Supply Chain and Third-Party Risk Management Platform*, August 4, 2022. https://www.carrickcapitalpartners.com/exiger-selected-as-government-wideenterprise-supply-chain-and-third-party-risk-management-platform.

[44] Mayer, Marina. “Single-Click Supply Chain Risk Detection SaaS Platform.” *Supply & Demand Chain Executive*, March 31, 2022. https://www.sdcexec.com/safety-security/riskcompliance/news/22144507/exiger-singleclick-supply-chain-risk-detection-saas-platform.

[45] “MAS ITC Contract Number: GS-35F-0292U.” https://www.gsaadvantage.gov/ref_text/GS35F0292U/0XY2JF.3TOFE6_GS-35F0292U_CSIEGSFSSPRICELISTPA57.PDF.

[46] “What Is Vendor Risk Management Software?” *Exiger*, November 11, 2022. www.exiger.com/perspectives/what-is-vendor-risk-management-software/.

[47] “Decision Science for National Security.” *Govini*, January 18, 2022. https://govini.com/decisionscience/.

[48] “National Security Knowledge Graph.” *Govini*, December 3, 2021. https://govini.com/techologies/national-security-knowledge-graph/.

[49] “Ark.Ai Applications.” *Govini*, March 21, 2023. https://govini.com/ark-applications/.

[50] “MAS Contract Number: 47QTCA23D0063.” GSA Advantage. https://www.gsaadvantage.gov/ref_text/47QTCA23D0063/0Y3H6Y.3TTU1M_47QTCA23D0063_GOVINI FSS.PDF.

[51] “Supply Chain & Logistics.” *Govini*, January 15, 2023. https://govini.com/applications/supply-chainlogistics/.

[52] “Ark.Ai - Find America’s Edge.” *Ark.Ai - Find America’s Edge*, https://ark.ai/. [53] “Enterprise Operational Resilience & Supply Risk Solutions.” *Interos*, May 16, 2023. www.interos.ai/about/.

[54] “Commercial Data Sheet - November 2019.” Interos, November 2019.

[55] “Interos Advances Industry-First Operational Resilience Score, Adding Early Warning Cyber Behavior Model to Identify Which Suppliers Are Most Vulnerable to Urgent Threats.” *Interos*, March 9, 2023. www.interos.ai/press/interos-advances-industry-first-operational-resilience-score-adding-early-warningcyber-behavior-model-to-identify-which-suppliers-are-most-vulnerable-to-urgent-threats/.

[56] “Product Overview - Interos.” *YouTube*, YouTube, August 12, 2021. https://www.youtube.com/watch?v=D74sT70vHtA&t=1s.

[57] “Supply Chain Risk Management Technology.” *Interos*, www.interos.ai/why-interos/, Accessed February 6, 2023.

[58] “Product Overview - Interos.” *YouTube*, YouTube, August 12, 2021. https://www.youtube.com/watch?v=D74sT70vHtA&t=1s.

Written by:

General Services Administration (GSA)
Federal Acquisition Service (FAS)
Information Technology Category (ITC)
Jeannette Grover
Julius White
Marie Rivera
Priscilla Giannelli
Jesse Autry

LMI
Beatrix Boyens
Jon Amis

MetaPhase Consulting Group (MPC)
Andrew Papp
Katie Caulfield
Juni Kim

Acknowledgments

The authors would like to acknowledge and thank Jon Boyens of the National Institute of Standards and Technology (NIST), Angela Smith (NIST), Tom Smith (GSA), Mohammad Abul-Hawa (GSA), Albert Ingram (GSA), Dody Brownridge (GSA), Roy Holland (GSA), Tammy Stathas (GSA), Wayne Thomas (GSA), Michael Harris (LMI), Mark Bronson (LMI), and the LMI creative and editorial team for their contributions.