Audit of the Department's Cyber Supply Chain Risk Management Efforts

★ ★ ★

AUDIT DIVISION

22-087

JULY 2022

EXECUTIVE SUMMARY

Audit of the Department's Cyber Supply Chain Risk Management Efforts

Objective

The Department of Justice (Department or DOJ) Office of the Inspector General (OIG) conducted this audit to determine the extent to which the DOJ, through the Justice Management Division (JMD) and the Federal Bureau of Investigation (FBI), implemented an organizational supply chain risk management program that identifies, assesses, mitigates, and responds to supply chain risk throughout the information technology (IT) lifecycle.

Results in Brief

Cyber supply chain risk is the potential for harm or compromise that arises as a result of cybersecurity risks from suppliers, their supply chains, and their products or services. Managing such risk is referred to as Cyber Supply Chain Risk Management (C-SCRM). DOJ currently operates two distinct C-SCRM programs—one operated by and focused on the FBI; and a second operated by JMD that is focused on all non-FBI Department components.

Overall, JMD lacked the personnel resources to effectively manage its C-SCRM program, resulting in widespread noncompliance, outdated C-SCRM guidance, inadequate threat assessments, and insufficient mitigation and monitoring actions. These weaknesses increase the risk of introducing products or services into DOJ's IT environment that could compromise the integrity of its systems and data. While the FBI's program is more modern than JMD's, it too has several processes and deliverables in need of enhancement. In fact, we found that FBI procurement officials often improperly bypassed its C-SCRM program entirely, due in part to a misunderstanding or unawareness of the C-SCRM requirements.

Recommendations

Our report contains a total of 17 recommendations, specifically to JMD, the FBI, and the Drug Enforcement Administration (DEA). We requested responses to our draft audit report, which can be found in Appendices 4 through 7. Our analysis of those responses is included in Appendix 8.

Audit Results

Federal agencies increasingly rely on commercially available technology solutions to fulfill their missions and support their critical functions. This, in addition to globalization, outsourcing, and increased digitization, has resulted in complex, diverse, and extensive IT supply chains. These conditions create numerous cyber supply chain risks that federal agencies must manage. C-SCRM aims to identify and assess susceptibilities, vulnerabilities, and threats throughout the supply chain and develop mitigation strategies to combat those threats.

C-SCRM Non-Compliance by DOJ Components and a Lack of Resources to Effectively Manage its Program

At the time of our review, JMD had only one individual tasked with managing its C-SCRM program. To implement its C-SCRM program, JMD relies on Department components to independently attain knowledge of the DOJ's C-SCRM requirements and to develop procedures and internal controls to implement them on their own. However, JMD's primary C-SCRM guidance did not include any monitoring and oversight provisions and JMD had not taken steps to ensure Department components were compliant with its requirements. We assessed C-SCRM compliance by several of the largest non-FBI DOJ components—Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF); DEA; Executive Office for U.S. Attorneys (EOUSA); Federal Bureau of Prisons (BOP) and Federal Prison Industries, Inc. (FPI); the Justice Management Division (JMD); National Security Division (NSD); and U.S. Marshals Service (USMS). We concluded that only ATF and the DEA were compliant with the JMD C-SCRM requirements, including submitting applicable IT purchases for a C-SCRM review.

Overall, JMD lacked the personnel resources necessary to effectively manage this critical program. JMD needs to provide communication, outreach, and training to Department components and develop procedures to

periodically assess their efforts. Without such efforts, C-SCRM controls could be bypassed and high-risk IT could be installed without JMD authorization or a risk mitigation plan.

JMD Should Ensure that its C-SCRM Program is Current and Comprehensive to be Most Effective

We found that JMD's C-SCRM guidance needs to be updated and consolidated, and that JMD should periodically re-assess the Department's systems to prioritize those which are most vulnerable and that would cause the greatest organizational impact if compromised. We also determined that JMD could enhance its C-SCRM program by examining the vulnerabilities, likelihood, and impact of a supply chain event; assessing IT resellers; developing effective risk mitigation steps; and evaluating its C-SCRM program needs.

The Drug Enforcement Administration Should Develop a C-SCRM Program as Required by an Intelligence Community Directive

DEA had established a policy-driven requisition process that flagged and submitted purchase requests for C-SCRM assessment in accordance with JMD requirements. However, the DEA's Office of National Security Intelligence (ONSI) is a member of the U.S. Intelligence Community and subject to additional criteria to protect the supply chain. We determined that ONSI had not established a supply chain risk management program as required by an Intelligence Community directive. Instead, ONSI followed JMD's less stringent C-SCRM procedures. Without such a program, ONSI may not be sufficiently managing risk to the integrity, trustworthiness, and authenticity of its mission-critical U.S. Intelligence Community products and services.

FBI's Procurements Appear to Often Bypass the C-SCRM Process, Thereby Increasing Risk

For the FBI's C-SCRM process to be effective, it must ensure that the applicable information and communications technology (ICT) and classified service purchase requests are properly identified and subjected to the required assessment procedures. According to FBI data, between October 2017 and May 2021, hundreds of millions of dollars in requisitions (transactions over $10,000) may have improperly bypassed the C-SCRM process. Furthermore, FBI purchases of $10,000 or less (using government purchase cards) also appeared to bypass the C-SCRM process, but to an unknown extent, given the FBI's lack of a mechanism to monitor whether bypasses were occurring. Purchases that improperly bypass the C-SCRM process may not receive mitigation steps to address the identified risks, thereby increasing supply chain risk throughout the FBI.

FBI Can Improve Elements of its C-SCRM Program

FBI's C-SCRM efforts are primarily shared between its Acquisition Security Unit (ASU) and Supply Chain Risk Management Unit (SCRM Unit). ASU conducts vendor threat assessments to determine if the companies offering ICT goods and services present risks to the FBI. The SCRM Unit completes product vulnerability assessments to identify the risks associated with specific products, and then summarizes all vendor and product risks related to a procurement.

FBI has made significant progress towards modernizing and operating its C-SCRM program, but there remain several areas of improvement. Specifically, ASU had not incorporated threat rating criteria and sourcing standards into its vendor threat assessments, as required by Intelligence Community directive; and should modify its vendor threat assessment process to better align its information collection methodology, risk tolerance levels, and other attributes with the enterprise needs. Additionally, the SCRM Unit needed to improve its key deliverables to better align with Intelligence Community requirements and enhance both its risk mitigation and continuous monitoring efforts.

FBI Could Better Integrate C-SCRM Across the Organization

Managing cyber supply chain risk is a complex undertaking that requires a coordinated interdisciplinary approach. FBI's C-SCRM program requires, incorporates, or has a nexus to several other FBI components including Finance Division for the government purchase card program and requisitions by Contracting Officers; the Operational Technology Division; and FBI investigative and intelligence divisions. The challenge is synthesizing all of these efforts into a comprehensive C-SCRM program, which the FBI lacked. The FBI could benefit from better integrating C-SCRM across the organization, such as through the establishment of a Program Management Office.

Other JMD and FBI Noncompliance & Areas of Improvement

JMD and the FBI were non-compliant with a congressional requirement to conduct C-SCRM reviews for new Federal Information Security Modernization Act of 2014 (FISMA) reportable IT systems that the Department designated high- or moderate-impact. Lastly, JMD and the FBI need to better share C-SCRM information within the Department, bolster information sharing with other federal agencies, and access and contribute to an Intelligence Community repository.

Table of Contents

Introduction

Federal agencies, like DOJ, increasingly rely on commercially available technology solutions to fulfill their missions and support their critical functions. However, globalization, outsourcing, and digitization have resulted in complex, diverse, and extensive information technology (IT) supply chains that leave federal agencies with less control and visibility into their supply ecosystems. Such conditions create numerous cyber supply chain risks that federal agencies must manage. For instance, the "SolarWinds" intrusion highlighted the risks associated with software supply chains throughout the federal government and the private sector alike, having resulted in the exposure and presumed theft of unclassified email content from approximately 3 percent of the email accounts within DOJ alone.[1] In addition to the harm caused to the Department, thousands of other public and private sector entities were also affected.[2] Considered by many to be among the worst intrusions of government and private networks in U.S. history, it is but the latest in a long line of supply chain-related compromises in recent years.[3]

KEY TERMS

Cyber Supply Chain Risk is the potential for harm or compromise arising from suppliers, their supply chains, their products, or their services. Cybersecurity risks throughout the supply chain arise from threats that exploit vulnerabilities or exposures within products and services traversing the supply chain as well as threats exploiting vulnerabilities or exposures within the supply chain itself.

Cyber Supply Chain Risk Management (C-SCRM) is a systematic process for managing exposure to cybersecurity risks throughout the supply chain and developing appropriate response strategies, policies, processes, and procedures.

The multidisciplinary approach to managing cyber supply chain risks is called Cyber Supply Chain Risk Management (C-SCRM).[4] According to the National Counterintelligence and Security Center, while there is no single "silver-bullet" solution to combat supply chain threats, organizations can consider basic C-SCRM principles to enhance the resilience of their supply chains.

DOJ's C-SCRM Programs

The Department operates two different C-SCRM programs. One program is operated by and focused solely on the Federal Bureau of Investigation (FBI). The other is operated by the Justice Management Division (JMD) and covers all non-FBI Department components. These programs manage cyber supply chain risk by attempting to understand and address the threats and vulnerabilities posed by IT procurements, including computers, software, equipment, licenses, classified

---

[1] SolarWinds is a provider of information technology (IT) infrastructure management software that organizations use to monitor and manage the performance of their IT environments.

[2] According to the Justice Management Division (JMD), the "SolarWinds" intrusion was a sophisticated attack against a trusted IT vendor. While C-SCRM is an important element of a cybersecurity program, JMD stated that it would not have prevented the SolarWinds intrusion.

[3] Other recent supply chain-related compromises involved the delivery of malware through software updates; malware installed on new computers after they were shipped from a factory to a distributor, transporter, or reseller; and cryptocurrency schemes supported by software supply chain attacks.

[4] "C-SCRM," "ICT SCRM" (information and communications technology), and "SCRM" (used in an IT context), are often used interchangeably. We adopted the National Institute of Standards and Technology's (NIST) use of "C-SCRM," which NIST stated has evolved from a narrow focus on ICT supply chains to covering any cybersecurity-related supply chain risk.

services, drones, network devices, and radio systems. The basics of these C-SCRM programs are shown in Table 1.

Table 1

JMD & FBI C-SCRM Program Comparison

	Justice Management Division (JMD)	Federal Bureau of Investigation (FBI)
C-SCRM Program Establishment Date	2012	2005
Primary Responsibility for C-SCRM Program	JMD Cybersecurity Services Staff	FBI Acquisition Security Unit & Supply Chain Risk Management Unit
Components Subject to the C-SCRM Program	All non-FBI Department components	FBI only
C-SCRM Coverage	Limited *(see note)*	Extensive *(see note)*
IT Spending Subject to C-SCRM (FY 2020)	Not tracked by JMD	$2.2 billion
No. of C-SCRM Program Personnel (FY 2021)	1	29
No. of C-SCRM Vendor Threat Assess. (FY 2020)	129	1,053

Note: JMD's C-SCRM coverage was limited to IT acquisitions for certain product types and information systems. FBI's coverage was expansive, including all IT products and classified services.

Source: OIG, based on FBI and JMD information

Prior Reports

The U.S. Government Accountability Office (GAO) issued two reports in the past decade that assessed Department compliance with C-SCRM requirements. In 2012, GAO reported that while the Department had identified supply chain protection measures, it had not developed procedures for implementing and monitoring compliance. JMD concurred with the resulting GAO recommendation that the Department "develop and implement a monitoring capability to verify compliance with, and assess the effectiveness of supply chain protection measures."[5] In 2020, GAO reviewed 23 federal agencies to determine if they had

[5] GAO, *IT Supply Chain – National Security-Related Agencies Need to Better Address Risks*, GAO-12-361 (March 2012), https://www.gao.gov/assets/gao-12-361.pdf (accessed August 2021). GAO closed this recommendation, stating that the Department established a capability to monitor compliance with the policy by tracking assessments of supply chain security risks of vendor products. GAO report recommendations https://www.gao.gov/products/gao-12-361 (accessed June 9, 2021).

implemented foundational practices for managing cyber supply chain risks.[6] GAO issued recommendations to the Department (not including the FBI) to fully implement foundational practices in its organization-wide approach to C-SCRM. As of April 2022, the GAO recommendations to the Department remained open.

OIG Audit Approach

The objective of this audit was to determine the extent to which the Department, through JMD and the FBI, implemented an organizational supply chain risk management program that identifies, assesses, mitigates, and responds to supply chain risk throughout the IT lifecycle. Our audit generally covered, but was not limited to, Department C-SCRM activities from October 2016 through January 2022. To accomplish our objective, we:

- Interviewed Department officials and analyzed information from the FBI; JMD; Bureau of Alcohol, Tobacco, Firearms and Explosives; Drug Enforcement Administration; Executive Office for U.S. Attorneys; Federal Bureau of Prisons; National Security Division; and U.S. Marshals Service.
- Assessed the FBI's, JMD's, and other Department components' compliance with various C-SCRM policies and procedures.
- Reviewed FBI and JMD acquisition data to determine if applicable purchases were subjected to their C-SCRM programs.
- Evaluated the FBI's and JMD's C-SCRM implementation efforts, including their identification of applicable IT procurements, processes and deliverables, mitigating actions, and continuous monitoring.
- Examined the Department's C-SCRM efforts in the areas of information sharing and building program awareness.

Appendix 1 contains a more detailed description of our audit objective, scope, and methodology.

[6] GAO, *Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks*, GAO-21-171 (December 2020), https://www.gao.gov/assets/gao-21-171.pdf (accessed February 2021).

Audit Results

At the time of our review, JMD had only one individual tasked with managing its C-SCRM program and therefore lacked the personnel resources necessary to effectively manage this critical program. The lack of personnel has resulted in widespread noncompliance, outdated C-SCRM guidance, inadequate threat assessments, and insufficient mitigation and monitoring actions. These weaknesses increase the risk of introducing products or services into DOJ's IT environment that could compromise the integrity of its systems and data. While the FBI's program is more mature than JMD's and has 29 FBI staff members assigned, it too has several processes and deliverables in need of enhancement. In fact, we found that FBI procurement officials often improperly bypassed its C-SCRM program entirely, due in part to a misunderstanding or unawareness of the C-SCRM requirements. Further, both JMD and the FBI need to comply with congressional and external C-SCRM requirements and improve their information sharing efforts within the Department as well as with the U.S. Intelligence Community (USIC) and non-USIC federal partners.

Justice Management Division's C-SCRM Program

The Justice Management Division (JMD) is primarily responsible for implementing C-SCRM efforts for all non-FBI Department components.[7] In 2012, JMD began developing its C-SCRM program in response to congressional requirements and an audit performed by GAO.[8] JMD's efforts culminated in the issuance of its Procurement Guidance Document 14-03 (Procurement Guidance 14-03), in April 2014. Procurement Guidance 14-03 is the primary driver of JMD's C-SCRM program and includes: the types of IT acquisitions subject to C-SCRM; required clauses to be included in procurement solicitations; Contracting Officers' responsibilities; JMD's assessment of the national security risks posed by award; and the procedures for risk acceptance. Table 2 lists the IT acquisition types that are subject to JMD's C-SCRM procedures.

[7] JMD's C-SCRM efforts are led by its Cybersecurity Services Staff, located within JMD's Office of the Chief Information Officer. We refer to JMD when discussing these Cybersecurity Services Staff efforts.

[8] In FY 2012, Congress prohibited the Department from acquiring IT systems unless it first assessed the associated risk of cyber-espionage or sabotage and consulted the FBI about potential threats. Consolidated and Further Continuing Appropriations Act 2012, P.L. 112-55 § 518 (2011), https://www.congress.gov/112/plaws/publ55/PLAW-112publ55.pdf (accessed April 5, 2022). Congress has revised and reiterated these requirements each year from FYs 2013 through 2021.

Table 2

JMD's C-SCRM Requirements

C-SCRM Requirement For:	Department C-SCRM Policy	Example(s)
Equipment or software to be used in, on, or to support an existing or new national security system or a Department-wide IT system[a]	Procurement Guidance 14-03	Software/hardware used on Department components' classified systems
A new Federal Information Security Modernization Act (FISMA) reportable IT system that the Department designated high- or moderate-impact[b]	Procurement Guidance 14-03	Case management systems, general support systems, and data analytics systems
Wireless communication platforms	DOJ Memorandum on Acquisition of Wireless Communication Platforms	Land-mobile radio systems, drones, and counter-drone systems
Foreign-owned IT products must obtain a Department waiver, and the waiver process includes a C-SCRM assessment	DOJ Cybersecurity Standard, Unclassified Security Control Matrix	Software developed by foreign-based companies

[a] National Security System is defined in 40 U.S.C. § 11103 and includes systems which involve intelligence activities, cryptologic activities related to national security, or that are critical to an intelligence mission.

[b] A FISMA reportable IT system is an information system that supports the operations and assets of the agency. FISMA systems are categorized based on the potential impact on an organization, should certain events occur which jeopardize the information systems. The potential impact levels are high, moderate, and low.

Source: OIG analysis of JMD's C-SCRM requirements

If Department personnel receive a purchase request that falls within one or more of the categories listed in Table 2, they must submit to JMD: an intake form, a vendor-completed risk questionnaire, and information on any known espionage or sabotage vulnerabilities presented by the procurement.[9] The C-SCRM Program Manager then conducts a vendor threat assessment (formally known as a Supply Chain Risk Assessment) and upon completion, drafts a risk determination letter, documenting whether the IT acquisition is acceptable and listing any risk mitigating actions.[10] If acceptable, JMD submits the risk determination letter to the requesting component for final approval by its authorizing official.

A classified vendor threat assessment is the key component of JMD's C-SCRM process. Vendor threat assessments research the companies supplying the Department's most critical IT products for national security risks, including their key management personnel; foreign ownership, control, or influence concerns; strategic partnerships; existing or previous government contracts; and several other areas based on information from commercial and government sources, including FBI databases. JMD compiles this information, identifies any threat risk factors, and generates a final score of low, moderate, high, or critical. For

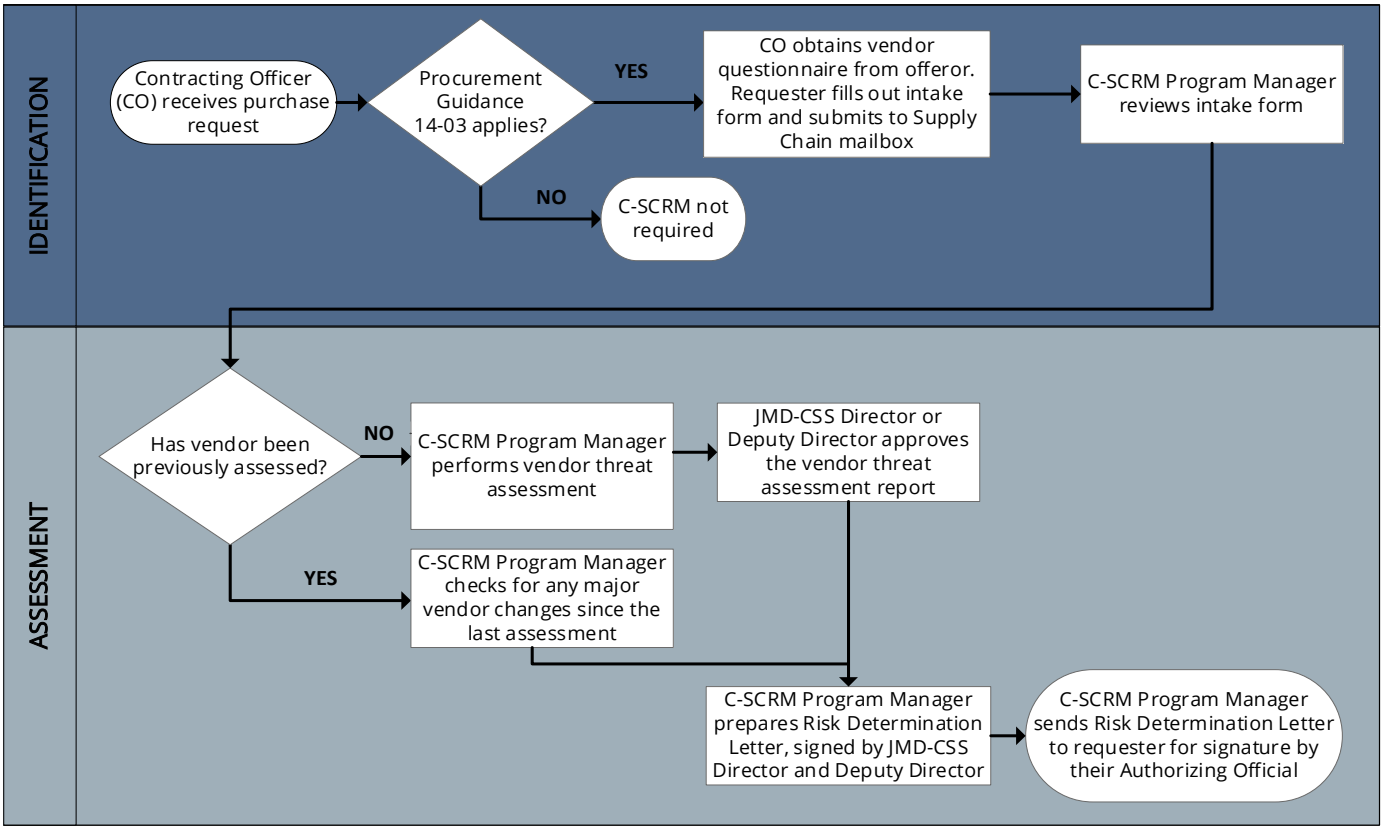
[9] This is part of the general compliance process under Procurement Guidance 14-03. However, compliance steps and form submissions vary depending on the particular C-SCRM requirement.

[10] A C-SCRM Program Manager is responsible for the overall coordination and execution of the C-SCRM program. This JMD official conducts vendor threat assessments, monitors the workflow of all C-SCRM requests, and periodically submits metrics to JMD leadership and Congress.

low, moderate, and high scores, JMD typically defers to the acquiring component to make the final determination of whether the identified risks, if any, are acceptable. However, for "critical" scores, JMD will deny the acquisition and the acquiring component must identify an alternative source. Figure 1 depicts JMD's C-SCRM review process.

Figure 1

JMD's C-SCRM Review Process (under Procurement Guidance 14-03)

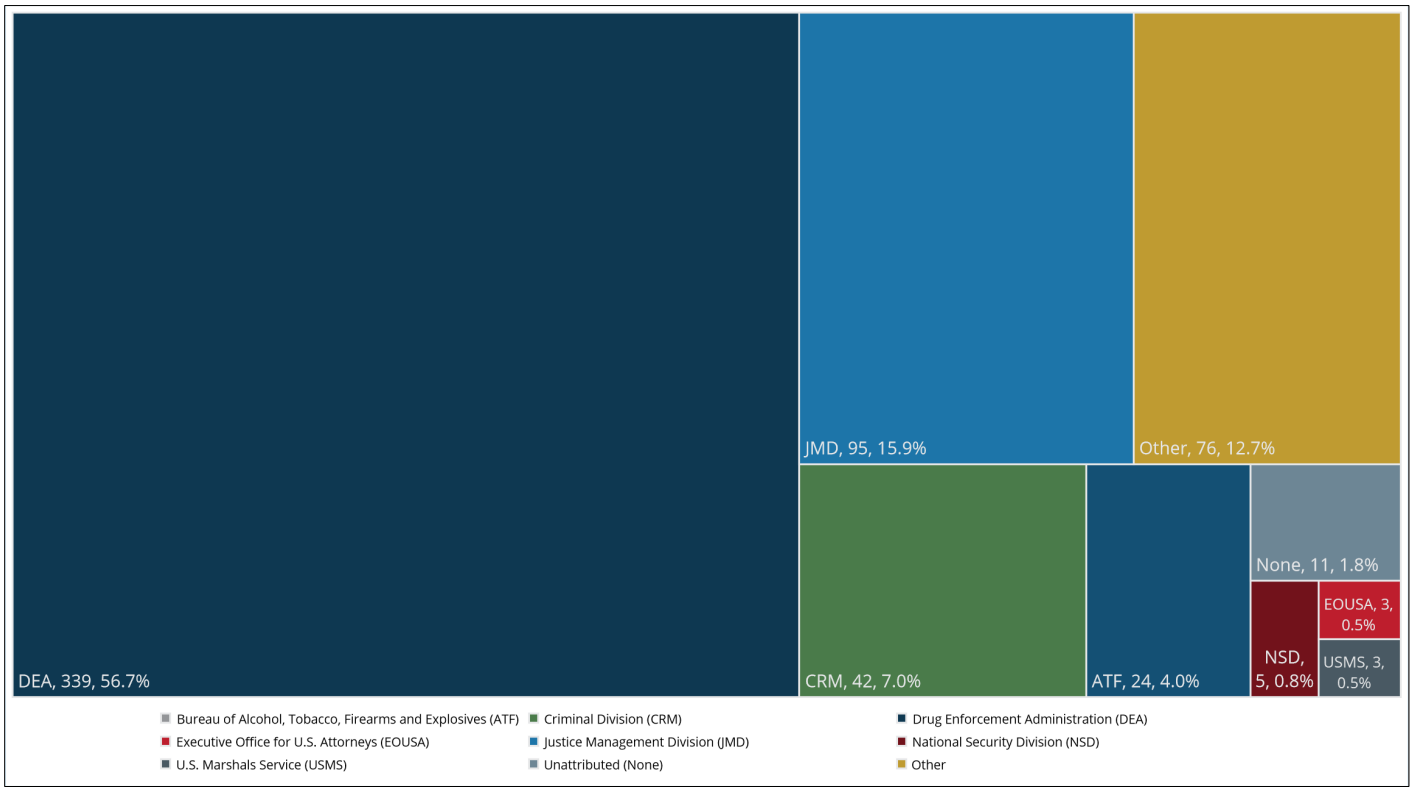


Source: JMD, adapted by OIG

As shown in Figure 2, from July 2015 through February 2021, JMD conducted 598 vendor threat assessments on behalf of Department components, or approximately 100 per year, covering an array of vendors offering IT products.

Figure 2

JMD Vendor Threat Assessment Requests
July 2015 through February 2021
(598 Total Requests Received)



Note: "Other" includes DOJ components not listed above and requests that included multiple DOJ components. "None" refers to assessments with no submitting Department component listed.

Source: OIG figure, based on JMD data

JMD Should Enhance its Monitoring of its C-SCRM Requirements to Ensure Department Compliance

For JMD's C-SCRM program to be effective, it must have assurance that Department components' applicable IT acquisitions are being identified so that the appropriate C-SCRM procedures can be applied. This is a challenge because JMD does not control, manage, or have full visibility into Department components' IT acquisitions. While Department components are ultimately accountable for following DOJ policies such as Procurement Guidance 14-03, we believe that JMD needs to proactively communicate and reiterate its requirements throughout the Department, provide guidance and training as necessary, and establish procedures to monitor Department components' compliance. Otherwise, Department components could inadvertently or improperly bypass the C-SCRM controls without JMD's knowledge and install high or critical-risk IT without JMD authorization or a risk mitigation plan.

As previously noted, JMD concurred with a 2012 GAO recommendation that it develop and implement a monitoring capability to verify compliance with and assess the effectiveness of its C-SCRM measures. JMD's primary C-SCRM policy, Procurement Guidance 14-03, does not include any monitoring and oversight provisions, and we determined that JMD had not taken steps to ensure Department components were compliant with its requirements. The C-SCRM Program Manager was not confident that JMD was receiving all applicable requisitions; did not have sufficient visibility to assess the program's overall coverage or the ability to determine whether acquisitions had circumvented the process; and did not oversee whether components were actually incorporating C-SCRM language into their requests for purchases, quotations, and invitations for bids. In the absence of such oversight, we determined that several Department components were not consistently submitting applicable IT purchases for a C-SCRM review in accordance with JMD requirements.

BOP/FPI, EOUSA, NSD, JMD, and USMS were not Compliant with C-SCRM Requirements

Senior JMD officials told us that while JMD leads the Department's C-SCRM program, other Department components are key enablers of the program's success and must provide support and accountability. To assess Department compliance with JMD's C-SCRM procedures, we interviewed and collected data and information from the following Department components: Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF); Drug Enforcement Administration (DEA); Executive Office for U.S. Attorneys (EOUSA); Federal Bureau of Prisons (BOP) and Federal Prison Industries, Inc. (FPI); the Justice Management Division (JMD); National Security Division (NSD); and U.S. Marshals Service (USMS).[11] We selected these Department components based on their organizational missions, annual IT spending, and JMD's C-SCRM assessment data. We examined whether each of these components acquired IT items that were subject to JMD's C-SCRM program. If so, we then assessed whether they had policies or procedures to identify and submit applicable requests to JMD and determined whether these components had been consistently submitting such requests. Table 3 summarizes our results.

[11] Federal Prison Industries, Inc. is a wholly owned government corporation and one of the Federal Bureau of Prisons' most important inmate work programs.

Table 3

Summary of Select Department Components' Compliance with JMD's C-SCRM Requirements

Department Component	No. of Vendor Threat Assessment Requests (July 2015 thru February 2021)	IT Purchases Subject to JMD C-SCRM Requirements?	Compliant with JMD C-SCRM Requirements?	Compliance Description
ATF	24	✓	✓	**Compliant.** Maintained implementation policies/procedures and systematically submitted requests.
DEA	339	✓	✓	**Compliant.** Maintained implementation policies/procedures and systematically submitted requests.
BOP/ FPI	0	✓	✗	**Noncompliant.** Did not maintain processes or procedures. No submissions.
EOUSA	3	✓	✗	**Noncompliant.** Did not maintain processes or procedures. Submissions were ad hoc.
JMD	95	✓	✗	**Noncompliant.** Did not maintain processes or procedures. Submissions were ad hoc.
NSD	5	✓	✗	**Noncompliant.*** Did not maintain processes or procedures. Submissions were ad hoc.
USMS	3	✓	✗	**Noncompliant.** Did not maintain processes or procedures. Submissions were ad hoc.

* As noted below, in response to our audit, NSD developed and issued an internal C-SCRM policy in October 2021.

Source: OIG table based on JMD data, and interviews and information from Department components

We concluded that while all of the above Department components had applicable purchases, only ATF and the DEA were compliant with the JMD C-SCRM requirements that we reviewed, having established policy-driven processes that flagged applicable purchase requests, and consistently submitting those items to JMD to undergo its C-SCRM process.[12] However, we found that the BOP and FPI, EOUSA, JMD, NSD, and USMS were noncompliant, having not maintained implementation procedures and not systematically submitting applicable IT purchases to JMD for C-SCRM review.

BOP and FPI had not submitted any vendor threat assessment requests to JMD over the nearly 6-year span, although they had applicable purchases, including $15 million for land-mobile radio systems and counter-drone systems during FYs 2020 and 2021 and two new FISMA reportable moderate-impact IT

[12] DEA Acquisition Policy Letter 2014-09 (May 2, 2019), *Risk Assessment Procedures for High- and Moderate-Impact IT System Equipment and Hardware (Revised)*. ATF Acquisition Management Policy No. 64A (August 2015), *Restrictions on the Use of Funds for the Acquisition of IT Systems – Procedures for National Security and Department-wide systems*. DEA and ATF also provided other documents evidencing their compliance.

systems in 2019. EOUSA submitted only three vendor threat assessment requests to JMD over the period, though its Chief Information Officer acknowledged that it should have submitted more, including foreign-owned IT and new FISMA reportable IT systems.[13] Neither BOP, FPI, nor EOUSA developed policies or procedures to implement JMD's C-SCRM requirements, though officials expressed plans to achieve compliance.

We determined that JMD had not implemented a systematic process to reliably identify its purchase requests subject to C-SCRM, but instead, according to the C-SCRM Program Manager, conveyed its requirements through word-of-mouth communication. Such an informal approach can result in compliance gaps. For instance, the C-SCRM Program Manager did not know whether JMD's Security and Emergency Planning Staff—which oversees two JMD national security systems whose IT purchases are subject to C-SCRM—knew of the requirements and did not recall receiving any assessment requests from them.[14] JMD, as the administrator of one of the Department's C-SCRM programs, should set an example to other Department components on how to comply with its requirements.

NSD had only submitted five requests for a vendor threat assessment over a nearly 6-year timeframe, accounting for under 1 percent of the Department's total assessments. This was despite NSD's management of two national security systems; and according to NSD's Chief Information Officer, NSD conducts 90 percent of its work in classified environments. We determined that NSD had not established a process to implement Procurement Guidance 14-03, and therefore NSD acquisition officials had not flagged and submitted IT purchase requests to JMD to undergo the C-SCRM review process before awarding or ordering $4 million in IT products and services for use in classified operating environments during FYs 2019 and 2020.[15] Senior NSD officials acknowledged that NSD needed to correct its non-compliance with Procurement Guidance 14-03, but noted that NSD mostly purchased IT through government-wide acquisition contracts that included some C-SCRM procedures.[16] JMD's C-SCRM Program Manager told us that while government-wide acquisition contracts may contain basic C-SCRM protections, they do not provide the same level of scrutiny as JMD's program. In response to our finding, NSD developed and disseminated an internal C-SCRM policy in October 2021. NSD's new policy reiterates much of the language and processes contained within Procurement Guidance 14-03, with some additional steps unique to NSD

[13] According to JMD records, EOUSA acquired one new FISMA reportable system between October 2016 and March 2021 that was designated moderate-impact. However, in November 2021, EOUSA informed OIG that it had been underreporting its FISMA reportable systems and upon further examination determined it had acquired and was operating 21 other FISMA reportable systems (20 moderate-impact systems and 1 high-impact) that were also subject to JMD's C-SCRM requirements.

[14] Subsequent OIG analysis determined that JMD's Security and Emergency Planning Staff had submitted one assessment request over the approximately 6-year timeframe.

[15] NSD had, in at least one instance, collected the vendor-completed risk questionnaire, as required by Procurement Guidance 14-03, Section V, but had not provided it to JMD as part of the C-SCRM assessment process.

[16] For instance, NASA SEWP (Solutions for Enterprise-Wide Procurement) is a government-wide acquisition contract that offers information and communications technology and audio-visual products and services for federal agencies. NASA SEWP includes some C-SCRM contract clauses and procedures, such as an Established Authorized Reseller Program which restricts non-established authorized resellers from quoting items to customers. However, use of the reseller program is optional.

personnel. NSD informed us that it planned to review its compliance with this new policy in April 2022. Overall, NSD has taken prompt action to address its non-compliance with C-SCRM requirements.

USMS submitted only three vendor threat assessment requests to JMD over the approximately 6-year timeframe. USMS maintains a national security system with an over $20 million IT budget in FY 2021. We determined that the USMS had not been submitting any of this system's IT purchases for C-SCRM review in accordance with Procurement Guidance 14-03, and it had not established internal controls to identify and ensure that other applicable IT acquisitions underwent the C-SCRM assessment process. USMS officials explained that they could not comply with JMD requirements for their national security system because JMD did not have the framework, processes, and methods to address USMS's national security and law enforcement sensitive requirements; and that USMS believed it already had a more robust, though undocumented, C-SCRM program. USMS officials told us that to ensure compliance with JMD's C-SCRM program going forward, the USMS intended to develop its own JMD-approved C-SCRM program for its national security system and also follow JMD's existing procedures for all other applicable IT procurements.[17]

Based on the results of these major Department components, we believe there likely are other Department components that have not established the necessary procedures or controls to ensure compliance with JMD's C-SCRM program requirements. Without such procedures or controls, the Department increases the risk of introducing products or services into its IT environment that could compromise the integrity of its systems and data.

The IT Acquisition Review Process Could Help JMD Monitor Department C-SCRM Compliance

The Federal Information Technology Reform Act requires that each federal agency's Chief Information Officer maintain a significant role in all agency IT decisions. To ensure compliance with this Act, the Department developed its IT Acquisition Review process, which requires Department components (with the exception of the FBI) to report IT procurements to JMD's Office of the Chief Information Officer via an electronic form through an Intranet portal. Because the electronic form includes a question on whether C-SCRM is required, it provides JMD a centralized mechanism to monitor Department C-SCRM compliance. However, JMD was not obtaining and reviewing the IT Acquisition Review submissions for C-SCRM purposes. We identified several IT Acquisition Review submissions where a component marked an IT purchase request as requiring C-SCRM, but the request was approved despite not actually undergoing the C-SCRM process.

We believe JMD could use the IT Acquisition Review data to help monitor Department C-SCRM compliance. However, doing so would first require JMD update the electronic form to ensure the C-SCRM requirements are clear, comprehensive, and resolve existing policy inconsistencies. Specifically, the electronic form's current C-SCRM question is ambiguous, and the instructions are incomplete, as they do not inform users of all IT purchases subject to C-SCRM (i.e., wireless communication platforms and foreign-owned IT are omitted). Additionally, the JMD guidance excepts from the IT Acquisition Review process acquisitions tied to national security systems, despite the IT Acquisition Review's C-SCRM instructions indicating otherwise, making it unclear whether JMD wants users to report IT acquisition requests tied to national security

[17] Procurement Guidance 14-03 allows Department components to establish their own JMD-recognized C-SCRM programs, as long as they formally include mutual collaboration with the FBI.

systems.[18] JMD guidance also excepts from the IT Acquisition Review process, IT procurements below the $10,000 micro-purchase threshold. Because JMD's C-SCRM procedures apply to all applicable IT acquisitions, regardless of dollar amount, JMD would need to establish supplementary oversight controls to monitor Department compliance on IT acquisitions below the $10,000 threshold, such as when components acquire IT with a government purchase card. In 2020, JMD began planning to enhance the IT Acquisition Review form to improve the level of response and awareness of the C-SCRM requirements and to automatically identify IT acquisitions subject to C-SCRM. As of November 2021, a senior JMD official involved in the update anticipated implementing these and other changes by the end of 2021.

JMD Should Enhance Department C-SCRM Program Awareness

According to the National Institute of Standards and Technology (NIST), everyone within an organization has a role in managing cyber supply chain risk and should receive appropriate training to understand the importance of C-SCRM for their organization, their specific roles and responsibilities, and the processes and procedures for reporting incidents.[19] Individuals who have more significant roles in managing cyber supply chain risk should receive tailored C-SCRM training that helps them understand the scope of their responsibilities, the processes and procedures they are responsible for implementing, and what actions to take in case of an incident, disruption, or another C-SCRM related event. JMD conducted very limited outreach and training for its C-SCRM program.

As a result of the widespread Department non-compliance with JMD's C-SCRM Program, we believe JMD should enhance Department awareness of its C-SCRM program to ensure users understand the program's importance and are familiar with the required processes and procedures. This could be accomplished by integrating C-SCRM program information into an existing training, such as the cybersecurity awareness training that all users are required to complete, and then offering tailored C-SCRM training for those with more significant involvement in the process. In early 2022, JMD took steps to address this matter. Specifically, it provided a general overview of C-SCRM concepts within both its annual cybersecurity awareness training and its role-based IT professional training. JMD also stated that acquisition professionals will obtain C-SCRM awareness training from other sources, as appropriate.

To address these compliance, monitoring, and awareness concerns, we recommend that JMD coordinate with the BOP and FPI, EOUSA, JMD, NSD, and USMS, and other Department components that are subject to JMD's C-SCRM requirements and whose compliance statuses are unknown, to ensure they maintain or develop the procedures and controls necessary to comply with JMD's C-SCRM requirements; incorporate into its C-SCRM program, steps to monitor and verify Department compliance with its guidance through periodic outreach, communication, and the establishment of internal controls; and enhance Department awareness of its C-SCRM program, such as through training.

---

[18] DOJ Procurement Guidance Document 16-02, *Acquisition of IT Equipment, Software, and/or Services,* excepts acquisitions of IT used in, on, or to support a national security system from the IT Acquisition Review process. However, the IT Acquisition Review instructions state that national security system-related requests are subject to C-SCRM.

[19] The National Institute of Standards and Technology (NIST) is part of the U.S. Department of Commerce and its responsibilities include developing information security standards and guidelines, including minimum requirements for federal information systems.

JMD's C-SCRM Procedures Should be Updated and Consolidated

C-SCRM as a discipline has evolved significantly within the past decade and there is now an extensive array of often overlapping requirements, standards, guidance, best practices, and other resources available to organizations to help manage cybersecurity risks associated with their supply chains. See Appendix 2 for a list of notable federal C-SCRM guidance. During our work, several Department officials commented on the need for JMD to update its C-SCRM guidance—primarily Procurement Guidance 14-03—to be more current, comprehensive, and valuable. The following bullets describe JMD's existing guidance and potential improvements.

- **JMD's C-SCRM Guidance is Significantly Outdated –** C-SCRM is a dynamic environment that needs an adaptive framework to enforce. JMD issued its primary C-SCRM guidance (Procurement Guidance 14-03) over 7 years ago and has not updated it since. In the Consolidated Appropriations Act for FY 2016, Congress instructed the FBI to develop best practices for C-SCRM and stated that the Department "shall incorporate such practices into their [IT procurements] to the maximum extent practicable." FBI issued the required best practices document in 2016. JMD officials told us that JMD believed it was already addressing most of the practices described in the FBI document. However, JMD provided no evidence that it had assessed the document and incorporated any newly suggested practices into Procurement Guidance 14-03 or its other C-SCRM guidance, as required by Congress. During our audit, JMD also had not incorporated into its guidance NIST Special Publication 800-53, Revision 5's new C-SCRM control family requirements, such as employing controls to limit harm from potential adversaries identifying and targeting the organizational supply chain; and establishing agreements and procedures with entities involved in the supply chain.[20]

- **C-SCRM Requirements Should be Consolidated into a Single Procedure** – During the course of our audit, we learned of two C-SCRM requirements that were not included in JMD's primary guidance document. First, the Department prohibits the purchase of foreign-owned IT products without a waiver approved by the Chief Information Officer. Before obtaining this waiver, JMD must conduct a vendor threat assessment. Second, in October 2018, JMD instructed Department heads and Chief Information Officers to ensure that all wireless communication platforms follow the supply chain risk assessment process.[21] We believe it would be beneficial to both JMD and Department components responsible for compliance to consolidate these requirements into a single procedure in JMD's primary guidance document. See Table 2 for JMD's C-SCRM requirements.

- **JMD Should Periodically Re-assess the Department's Systems for Supply Chain Risk** – According to the NIST, organizations should tailor their C-SCRM plans to ensure that operations are able to adapt to constantly evolving threats; and to be responsive to changes within their own organization,

---

[20] NIST Special Publication 800-53 Revision 5 Security and Privacy Controls for Information Systems and Organizations https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf (accessed March 2022). NIST 800-53, Revision 5 is NIST's flagship security and privacy document for protecting organizations and systems across 20 families of controls, including Supply Chain Risk Management.

[21] Wireless communication platforms include, but are not limited to, all land-mobile radio systems, drones, counter-drone systems, and unmanned ground vehicles that are capable of processing, storing, or transmitting information. Land mobile radio is further defined in *Procurement Guidance Document 16-02, Acquisition of IT Equipment, Software, and/or Services*.

programs, and the supporting information systems.[22] Many of JMD's vendor threat assessments have been tied to national security systems. While protecting these systems is of significant importance, the SolarWinds breach demonstrated that the exploitation of unclassified networks can still cause substantial organizational harm, having potentially exposed the Department's information in the areas of law enforcement, national security, investigations, litigation, IT operations and infrastructure, and human resources. JMD could benefit from periodically re-assessing the Department's systems to identify and prioritize those which are most vulnerable and that would cause the greatest organizational impact if compromised; and depending on the results, update JMD's guidance.

- **Other Department Comments & Concerns about JMD's C-SCRM Program –** Department officials shared comments and concerns about JMD's C-SCRM program. Some suggested that JMD more transparently communicate its assessment processes and results, and information on JMD's risk tolerance, so they could better understand JMD's approach and any identified threats. Officials also questioned the value of certain C-SCRM processes, such as the vendor-completed risk questionnaire, which they characterized as a biased and uncorroborated document. Additionally, one Department official observed that Procurement Guidance 14-03's narrow emphasis on *new* FISMA reportable systems designated high- or moderate-impact may represent a gap, as it would not apply C-SCRM procedures to *existing* high- or moderate-impact FISMA reportable systems that had undergone changes and updates. Another Department official noted that the C-SCRM requirement for wireless communication platforms was not well-defined and that there should be greater JMD consideration of how such IT would be used. We found that JMD's C-SCRM procedures were generally the same, regardless of the nature of the IT acquired, the Department component that was acquiring it, and how or where it would be used or installed.

In April 2022, JMD published a C-SCRM strategy for FYs 2022 – 2024.[23] This new strategy: (1) provides an overview of the Department's C-SCRM program throughout the IT lifecycle; (2) consolidates several C-SCRM requirements (though it does not include the C-SCRM requirement for wireless communication platforms); (3) establishes roles and responsibilities for key personnel involved in the C-SCRM process; and (4) details C-SCRM training offerings. We believe JMD's strategy is a significant step towards enhancing its C-SCRM program.

We recommend that JMD's C-SCRM strategy consolidates the existing requirements, including for wireless communications platforms; is refreshed periodically to reflect the latest requirements, standards, and best practices; includes a periodic re-assessment of the Department systems that are most vulnerable or that would cause the greatest organizational impact if compromised; and includes processes that better promote transparency and communication of C-SCRM results to Department components.

---

[22] National Institute of Standards and Technology, Special Publication 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations https://csrc.nist.gov/publications/detail/sp/800-161/final (accessed November 23, 2021). In May 2022, this publication was superseded by NIST 800-161 Revision 1.

[23] Department of Justice Information and Communication Technology Services Supply Chain Risk Management Program Strategy, Fiscal Year 2022 – 2024. Version 1.0 (issued on April 28, 2022).

Review of JMD's C-SCRM Deliverables

JMD's classified vendor threat assessment is its key C-SCRM deliverable. JMD uses the vendor threat assessment to research the companies supplying the Department's most critical IT products for potential national security risks, assigns a threat rating score, and either denies or approves the acquisition. As part of our analysis of JMD's C-SCRM program, we judgmentally selected a sample of 25 vendor threat assessments to determine if they were completed in accordance with Department policies and procedures. Our review determined that, with the exception of 7 of the 25 assessments completed during the COVID-19 pandemic, JMD's reviews generally followed Procurement Guidance 14-03 and its vendor threat assessment template; queried data and information from various sources, including FBI classified databases; utilized a threat matrix to assign classified risk ratings; sufficiently detailed the basis for its determination; typically conducted the assessments in a timely manner and updated them every 3 years, as required; and documented risk mitigations and recommendations.

For the vendor threat assessments completed during the COVID-19 pandemic, the C-SCRM Program Manager said the pandemic forced JMD into a maximum telework posture where they could not access classified FBI resources.[24] The seven JMD assessments completed during this timeframe were sparse, based solely on unclassified research, often directly from vendor websites and no longer used JMD's vendor threat assessment template. Because these were solely unclassified assessments, they did not contain vendor risk ratings accessible only on classified systems. FBI had continued to conduct its classified research during the COVID-19 timeframe, but JMD had not consulted the FBI for assistance to alleviate its access limitations during this period. The C-SCRM Program Manager informed us that JMD resumed its classified analyses in the spring of 2021. Notably, for one of the seven assessments that JMD performed remotely, it had not identified any reason to prohibit an acquisition from a particular vendor, while an FBI analysis of the same vendor had found significant issues, resulting in the FBI's Acquisition Security Unit recommending that the FBI deny acquisitions from the company.[25] A Department official suggested that when such discrepancies occur, the FBI and JMD should meet to address and resolve them.

Although the pre-pandemic assessments we reviewed were generally compliant with Department policies and procedures, our review of JMD's vendor threat assessments identified the following two areas of improvement.

[24] Procurement Guidance 14-03 states that JMD, in consultation with the FBI, will assess the national security risks posed by an award. This consultation consists of accessing FBI databases.

[25] As noted in the FBI Should Modify its Vendor Threat Assessment Process to Better Meet its Enterprise Needs section of this report, a denial recommendation from the FBI's Acquisition Security Unit does not mean the FBI will ultimately deny purchases from the company. In this particular instance, the FBI's Office of the Chief Information Officer subsequently authorized the purchase on the condition that the purchaser first apply mitigation strategies to reduce the supply chain risk.

- **JMD's C-SCRM Assessment Process Should Include Vulnerabilities, Likelihood, and Impact; and Evaluate Resellers –** According to both NIST 800-161 and the Committee on National Security Systems Directive 505 (CNSS Directive 505), C-SCRM risk assessments should review and analyze threats, vulnerabilities, and the likelihood and impact of a supply chain event (See Figure 3 for a depiction of this process). While JMD's C-SCRM program analyzed vendor-related threats, it did not examine vulnerabilities, and the likelihood and impact of an event. This was in part because, in 2013, JMD structured its program to mirror the FBI's, and at that time the FBI's vendor threat assessment was the primary deliverable, which JMD adopted. The C-SCRM Program Manager explained that JMD's primary guidance, Procurement Guidance 14-03, omitted analyses of vulnerabilities, likelihood, and impact because it predated both NIST 800-161 and CNSS Directive 505, which were issued in April 2015 and July 2017, respectively.[26] Without these elements, JMD's risk assessments would contain gaps, which would preclude the establishment of effective mitigation controls that are tailored to the risk assessment findings. Notably, the FBI has since adapted its C-SCRM program to leverage the NIST 800-161 risk management framework to include vulnerability assessments, and during our review, was in the process of incorporating likelihood and impact analyses into its procedures. We believe JMD should similarly evolve its C-SCRM risk assessments to include vulnerabilities, likelihood, and impact, to ensure compliance and consistency.

  Additionally, JMD's assessment process should include authorized resellers, as counterfeit IT goods represent a major supply chain risk (see textbox). We determined that JMD could benefit by developing procedures to help prevent the acquisition of counterfeit IT goods. Particularly, while JMD conducted threat assessments of manufacturers offering mission-critical hardware and software, it did not do so for resellers. By contrast, the FBI applies its vendor threat assessments to resellers because, FBI officials said, supply chain threats such as product manipulation and counterfeits also exist at the reseller-level. Senior JMD officials commented that it is important to differentiate between resellers that can and cannot access and handle IT goods. We recommend that JMD update its C-SCRM risk assessment methodology to assess vulnerabilities, likelihood, and impact, in accordance with NIST Special Publication 800-161, Revision 1 and CNSS Directive 505; and that its risk assessment also be applied to resellers, particularly those handling IT goods.

Foundational C-SCRM Practice: Vetting Resellers

One foundational C-SCRM practice, according to NIST, is to purchase IT goods directly from qualified original equipment manufacturers or their authorized distributors and resellers. Doing so can reduce cyber supply chain risk and help ensure that IT items are authentic and have not been tampered with or altered.

In 2018, a Department component purchased several network hardware items from an unknown and unauthorized reseller. When they received and attempted to register these items, component officials learned the items had already been used by other government agencies and commercial entities, including outside the U.S. A component official explained that they do not use previously owned or refurbished parts due to potential compromise. They therefore disposed of these network hardware items.

[26] The Committee on National Security Systems revised CNSS Directive 505 in November 2021.

- JMD Should Enhance its Risk Mitigation Steps and Establish Monitoring Procedures – According to NIST, after organizations have identified and assessed supply chain risks, they should develop, document, and monitor performance of mitigating actions. Mitigating actions should be tailored to the individual organization, program, and operational contexts. After JMD completes its vendor threat assessment, the C-SCRM Program Manager drafts and submits to the acquiring Department component a risk determination letter documenting the assessment outcome and required risk mitigating actions. JMD development and monitoring of effective mitigations is particularly important because it generally accepts the supply chain risk on applicable IT procurements, having only denied five acquisitions from October 2017 through March 2021. However, we determined that JMD's risk mitigating actions were insufficient. Specifically, every risk determination letter contained the same two standard mitigation requirements, regardless of the IT being procured, of the actual assessment rating, and of whether the stipulations were even applicable.[27] Department personnel familiar with the process believed JMD's risk determination letters used to be more descriptive and actionable. The C-SCRM Program Manager acknowledged that the risk determination letter contained the same two standardized requirements and agreed that this was an area needing improvement. Furthermore, JMD had not established internal controls to monitor whether Department components actually proceeded with the assessed IT acquisition and followed the mitigating actions stipulated within the risk determination letter. Therefore, we recommend that JMD develop policies and procedures that enable it to establish viable mitigation options that are descriptive, actionable, and tailored to the user environment and operational contexts, to be included in risk determination letters as needed; and that it establishes internal controls to monitor Department fulfillment of the mitigating actions.

JMD's Assessment of its C-SCRM Program Needs

We believe that one root cause of the issues described above was a lack of JMD personnel resources necessary to effectively manage the existing C-SCRM program. It was unrealistic for a single JMD employee to operate and maintain a comprehensive program that covers nearly the entire Department and whose effective operation requires policy development; training, awareness, and outreach; day-to-day implementation, including conducting vendor threat assessments; and monitoring/oversight responsibilities.

A sufficiently resourced C-SCRM program could provide the flexibility to apply more robust assessments when necessary, such as supplementing its vendor threat assessments with analysis of IT vulnerabilities, the likelihood of an adversary exploiting a vulnerability, and of the impact of a compromise and of mitigating and recovering from that compromise. JMD's existing workload will only continue to grow, given its concurrence with GAO's recommendations to fully implement foundational C-SCRM practices; a 2021

[27] The two standard mitigation recommendations were that Department components: (1) ensure their legal counsel reviews stipulations, end-user agreements and terms/conditions posed from the acquisition of open-source software, freeware, and shareware; and (2) ensure contracts include specific data protection language and that contractor support personnel have the requisite clearances and need to know. These stipulations were included for acquisitions that did not even involve open-source software, freeware, shareware, or contractor support personnel.

Executive Order's emphasis on enhancing software supply chains; new Federal Acquisition Security Council guidance; new NIST C-SCRM guidance; and DOJ plans to apply C-SCRM to high value assets.[28]

According to NIST, identifying resource needs and taking steps to secure adequate, recurring, and dedicated funding are essential and important activities that need to be built into the C-SCRM strategy and implementation planning effort, and is a critical key enabler for the sustainment of a C-SCRM program capability. NIST further highlights that organizations should identify and assess which type and level of resources are required to implement a C-SCRM program capability and perform the required C-SCRM processes on an ongoing basis.

JMD's then Cybersecurity Services Staff Director (who was also the Department's Chief Information Security Officer) acknowledged that this was an area needing improvement, and near the conclusion of our audit, JMD took steps to enhance its personnel resources. Specifically, in April 2022, JMD officials informed us that they had acquired three contractors to support the C-SCRM program. Additionally, the Department's FY 2023 budget request seeks two more positions to improve JMD's C-SCRM program.[29] Given JMD's recent and ongoing efforts to assess and address its C-SCRM program resource needs, we are not making a recommendation related to this matter, though we encourage JMD to periodically reassess the funding and personnel necessary to sustain and expand its C-SCRM program capabilities.

The Drug Enforcement Administration Should Develop a C-SCRM Program as Required by an Intelligence Community Directive

The majority of JMD's vendor threat assessments were conducted on behalf of the Drug Enforcement Administration (DEA) and we determined that the DEA had established a policy-driven requisition procedure that flagged purchase requests to undergo JMD's C-SCRM process. However, because the DEA's Office of National Security Intelligence (ONSI) is a member of the U.S. Intelligence Community (USIC), ONSI is also subject to a set of USIC criteria whose purpose is to protect the supply chain as it relates to the lifecycle of mission-critical products, materials, and services used by the USIC. Specifically, Intelligence Community Directive 731–Supply Chain Risk Management (IC Directive 731), dated December 2013, and its five associated Intelligence Community Standards (which we collectively refer to as "IC Directive 731"), establish and define C-SCRM requirements for USIC mission-critical products, materials, and services, to manage the risks to their integrity, trustworthiness, and authenticity; and to address the activities of foreign intelligence entities and any other adversarial attempts aimed at compromising and exploiting the USIC supply chain,

---

[28] Executive Order 14028, Improving the Nation's Cybersecurity, Section 4, https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity; and National Institute of Standards and Technology Special Publication 800-53, Revision 5 and Special Publication 800-161 Revision 1 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf (all accessed May 9, 2022). JMD officials told the OIG they planned to establish a future C-SCRM requirement for high value assets. High value assets, according to OMB Memorandum M-17-09 https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-09.pdf (accessed April 5, 2022), are those assets, Federal information systems, information, and data for which unauthorized access, use, disclosure, disruption, modification, or destruction could cause a significant impact to the United States' national security interests, foreign relations, economy, or to the public confidence, civil liberties, or public health and safety of the American people.

[29] DOJ FY 2023 Congressional Budget Submission for Justice Information Sharing Technology https://www.justice.gov/file/1493046/download (accessed May 6, 2022).

which may include the introduction of counterfeit or malicious items. See Figure 4 below for a list of IC Directive 731's requirements.

We determined that ONSI had not established a supply chain risk management program as required by IC Directive 731.[30] ONSI officials were unaware of IC Directive 731's requirements because they did not frequently purchase IT equipment. Instead, ONSI generally leases its Top-Secret information systems from the Defense Information Systems Agency, whom the DEA said conducts the C-SCRM-related procedures.[31] ONSI officials acknowledged however, that ONSI also acquires IT for use on non-leased classified systems that should have complied with IC Directive 731, but DEA followed JMD's less stringent C-SCRM procedures. ONSI informed us that in FYs 2020 and 2021, it spent approximately $46,702 on mission-critical IT acquisitions that were subject to IC Directive 731. While there was some overlap between IC Directive 731's and JMD's C-SCRM procedures, such as for threat analysis, IC Directive 731's requirements to assess criticality, vulnerabilities, likelihood, and impact were not covered in JMD's procedures. JMD's C-SCRM Program Manager correctly noted that its policy did not reference IC Directive 731, that JMD was not involved in the USIC's implementation of C-SCRM, and that responsibility for compliance with IC Directive 731 belongs to the DEA. Without an IC Directive 731-driven program, ONSI may not be sufficiently managing the risk to the integrity, trustworthiness, and authenticity of its mission-critical USIC products and services.

ONSI officials noted that it is a small office, accounting for 0.3 percent of the DEA's total workforce and is the smallest member of the USIC. Therefore, ONSI does not currently have the personnel, resources, or skillset necessary to establish its own program. IC Directive 731 makes clear that ONSI is ultimately responsible for establishing and resourcing a supply chain risk management program, but the directive also states that it "is intended to complement other supply chain risk management programs." While additional resources may be necessary to establish this program, the DEA may be able to share compliance responsibilities with JMD, such as by incorporating JMD's existing vendor threat assessment into the IC Directive 731 procedures (though modifications may be necessary).[32] It may also be beneficial for the DEA to consult the FBI about its C-SCRM program, which incorporates IC Directive 731; and to further contact the Office of the Director of National Intelligence's National Counterintelligence and Security Center—which oversees implementation of IC Directive 731—for advice and best practices on structuring the DEA's C-SCRM program to ensure relevant ONSI purchases comply with IC Directive 731.

In August 2021, ONSI officials said they had begun efforts to ensure compliance with IC Directive 731, including drafting a standard operating procedure, retroactively applying C-SCRM procedures to applicable IT items that had not been previously assessed, joining a National Counterintelligence and Security Center supply chain working group, and requesting access to a C-SCRM information sharing repository intended for USIC members. See the section titled C-SCRM Information Sharing Requirements for USIC Members for

---

[30] IC Directive 731, Section F(2)(a).

[31] The Defense Information Systems Agency plans, engineers, acquires, tests, fields, operates, and assures information-sharing capabilities, command and control solutions and a global enterprise infrastructure to support U.S. Department of Defense and national-level leadership.

[32] Earlier in this report we recommended that JMD update its C-SCRM risk assessment methodology to assess vulnerabilities, likelihood, and impact. Doing so would more closely align JMD's C-SCRM process with IC Directive 731 requirements.

additional information on this repository. We recommend the DEA establish policies and procedures to ensure ONSI compliance with Intelligence Community Directive 731 and its associated standards.

Federal Bureau of Investigation's C-SCRM Program

As noted above, the FBI operates its own C-SCRM program. FBI's program began in 2005 when it tasked its Security Division (SecD) with addressing FBI compliance with a USIC directive to ensure that certain acquisitions were shielded from foreign exploitation. SecD's Acquisition Security Unit (ASU) was assigned responsibility for this mandate. ASU works to safeguard FBI operations and information through the proactive identification, assessment, and mitigation of risks associated with the procurement of critical assets and classified service contracts.[33] ASU fulfills this mission by conducting analytic reviews of companies for which the FBI has entered into contractual relationships. The analytic review is called a vendor threat assessment and uses publicly available and classified sources to examine a vendor's key management personnel; financial condition; foreign ownership, control, or influence concerns; criminal and counterintelligence concerns; and other matters.[34] Vendor threat assessments are classified documents maintained in Sentinel, the FBI's automated case management system. In FY 2021, ASU had a staff of 14 FBI employees and contractors conducting these assessments, and between FYs 2017 and 2021 ASU completed an average of 1,058 vendor threat assessments per year.

In September 2016, the FBI identified C-SCRM as a compliance risk due to the volume of IT procurement requests, the severity of possible failure points, and the potential consequences of failure. FBI's Acting Chief Information Officer told us that the FBI's C-SCRM risk assessment process, at that time, was too static and so heavily driven by whether an IT procurement had a foreign nexus that it resulted in a heap of products with the same high-risk rating but no means to differentiate them and make decisions along a spectrum of risk. In 2018, the FBI began transferring select C-SCRM responsibilities from SecD to the Office of the Chief Information Officer (OCIO), and in April 2019 created OCIO's Supply Chain Risk Management Unit (SCRM Unit), effectively splitting the FBI's C-SCRM program between SecD and OCIO. The SCRM Unit's mission is to identify and understand the threats and vulnerabilities of IT procurements for the FBI. The SCRM Unit executes its mission by creating product vulnerability assessments, which aim to identify the risks associated with specific products and to include the appropriate measures to reduce that risk.[35] In FY 2021, the SCRM Unit had 15 FBI employee and contractor positions; the SCRM Unit completed 1,362 product vulnerability assessments from January 2020 through March 2021.

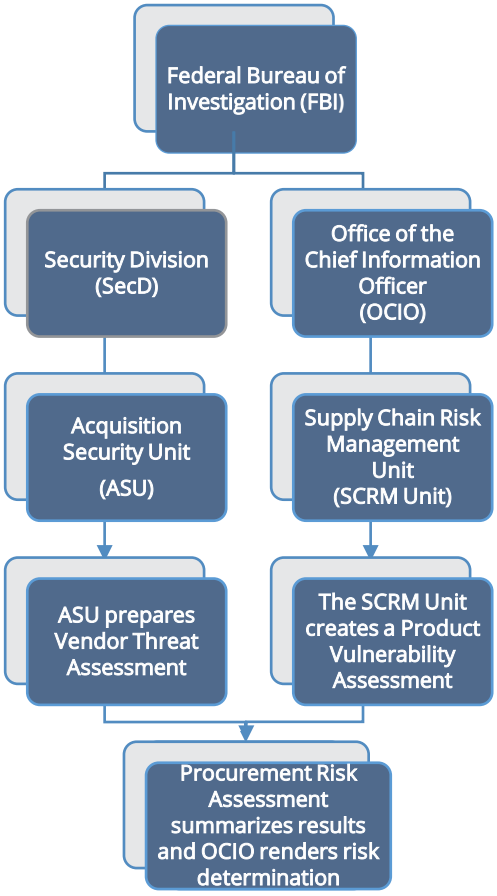
---

[33] Classified service contracts are any contract in which the contractor or its employees must have access to classified information during contract performance.

[34] ASU formally refers to its vendor threat assessments as "Company Threat Assessments." FBI's vendor threat assessments are similar to, and the basis for, the assessments performed by JMD, which were described in the Justice Management Division's C-SCRM Program section of this report.

[35] The SCRM Unit formally refers to its product vulnerability assessment as an Information Technology Risk Assessment Product.

FBI's C-SCRM program was applied to acquisitions of information and communications technology (ICT) items (hardware, software, communication items) and classified service contracts. For applicable acquisitions, ASU's vendor threat assessment analyzed the associated company and assigned a risk rating of either low, medium, high, or critical. ASU concluded the process by recommending approval or denial of the vendor, obtaining SecD supervisory approvals when necessary, and submitting its results to the SCRM Unit. If the SCRM Unit determined that an ICT procurement contained a particular product type or attribute, it conducted a product vulnerability assessment.[36] The SCRM Unit's product vulnerability assessment was paired with ASU's vendor threat assessment to create the procurement risk assessment, which is the summary document of the company and product risks associated with a procurement and used to grant final completion of the C-SCRM process. The SCRM Unit completed 6,391 procurement risk assessments from April 2019 through March 2021. The Unit Chief of the SCRM Unit and OCIO's Authorizing Official are responsible for reviewing and accepting or denying IT risk on behalf of the FBI.[37] These officials either: (1) unconditionally accept the IT risk, granting the requester authorization to proceed with the purchase; (2) conditionally accept the IT risk, granting purchase authorization on the condition that the requester follows OCIO-prescribed mitigation or risk-response actions, or (3) deny the IT procurement and/or re-direct the requester to an alternative product.[38]



FBI's Procurements Appear to Often Bypass the C-SCRM Process, Thereby Increasing Risk

NIST states that integrating C-SCRM principles into acquisition activities is essential to improving management of cyber supply chain risk at every step of the procurement and contract management process. For the FBI's C-SCRM process to be effective, it must ensure that the applicable ICT and classified service purchase requests

---

[36] As detailed in the FBI SCRM Unit's Product Vulnerability Assessments section of this report, from FYs 2020 through 2022, the SCRM Unit adjusted its application of the product vulnerability assessment to different ICT, based on product type or other attributes. In some instances, the SCRM Unit would not complete a product vulnerability assessment and instead proceeded to creating the procurement risk assessment.

[37] An Authorizing Official is a federal official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations, organizational assets, individuals, other organizations, and the nation. OCIO's Authorizing Official accepts or denies IT risk on the procurement risk assessments whose risk is deemed most critical, while the Unit Chief of the SCRM Unit handles all others.

[38] For classified service requisitions, ASU is fully responsible for the C-SCRM process and completes both the vendor threat assessment and the procurement risk assessment. A product vulnerability assessment is not necessary. Nor is OCIO involved in this process.

are properly identified and subjected to the C-SCRM assessment procedures (described in the section titled Review of the FBI's C-SCRM Deliverables).

Automated Requisition Tool

FBI ICT and classified service purchases over $10,000 are processed through the FBI's Automated Requisition Tool, which allows an end user to enter a requisition and send it through the approval chain and finally to the Contracting Officer for processing and acquisition. The Acquisition Security Unit's (ASU) Unit Chief is tasked with ensuring that all acquisitions involving critical components or classified services receive a completed vendor threat assessment. As long as the user submitting the requisition specifies that it involves an applicable product or service, an automated workflow transfers the requisitions into a C-SCRM module where ASU and the SCRM Unit initiate their reviews. ASU's involvement in this process consists of the following two steps.

1. **Acquisition Security Questionnaire** - ASU must review user-created requisitions to determine whether C-SCRM assessments are required. ASU accomplishes this task by ensuring that the requester properly completed an Acquisition Security Questionnaire that details the nature of the requisition. When applicable goods or services are identified by the requester, a checkbox is automatically selected, notifying ASU and the requester that this requisition will later be subject to C-SCRM procedures.

2. **Acquisition Security Request -** The requisition is then routed to budget and finance officials and eventually assigned to a Contracting Officer. If C-SCRM procedures are required, Contracting Officers must complete an Acquisition Security Request to input all the vendor and product information necessary for ASU and the SCRM Unit to commence their assessments. The Contracting Officer electronically submits the completed Acquisition Security Request to the C-SCRM module.

As part of this audit, the FBI generated a "bypass report" that identified requisitions for ICT products and classified services that ASU flagged for C-SCRM review (Step 1), but whose Contracting Officer purchased the products or services without completing the Acquisition Security Request (Step 2), thereby circumventing the C-SCRM process. This bypass report indicated that between October 2017 and May 2021, hundreds of millions of dollars in ICT goods and classified service acquisitions may have improperly bypassed the C-SCRM process.[39] To assess the reliability of this FBI data, we analyzed a judgmental sample of 20 requisitions that appeared to bypass the C-SCRM process. We found that 18 of the 20 requisitions (90 percent) had indeed improperly bypassed the C-SCRM process, as FBI officials were not able to provide a current procurement risk assessment from either the SCRM Unit or ASU for those requisitions.[40] Furthermore, 3 of the 18 bypassed requisitions were from vendors for which ASU had issued a "critical"

[39] Bypassed requisitions included licensing agreements; classified services; software; network equipment; and bulk hardware purchases.

[40] Two requisitions were "not applicable." One because it was canceled without purchase. The other was equipment purchased on behalf of a foreign law enforcement partner and C-SCRM is not required for IT products used outside of the FBI. For several of our sampled requisitions, the FBI maintained procurement risk assessments for similar requisitions from prior years. However, ASU officials explained that this was not an acceptable practice as each applicable requisition should be independently assessed. ASU attributed this to confusion among purchasing officials, and not intentional. Nevertheless, we considered such instances to be an improper bypass of the C-SCRM process.

rating and had recommended procurement denial. While this bypass report raises important concerns about ICT products and classified services improperly circumventing the FBI's C-SCRM process, it also contains data limitations that made it difficult to quantify and characterize the overall risk and impact of these bypasses. This was because the bypass report contained an unknown number of requisitions to incrementally fund existing classified service contracts that, even if bypassing the C-SCRM process, did not result in any supply chain risk to the FBI.[41]

FBI contracting personnel generally agreed about the importance of consistently submitting applicable requisitions through the C-SCRM process. They told us that several factors may have led to bypasses, including unfamiliarity with the C-SCRM requirements; efforts to avoid the often lengthy C-SCRM process; and to expedite the processing of requisitions, especially at the end of the fiscal year, or due to heavy workloads resulting from significant contracting personnel turnover in recent years. Additionally, while the C-SCRM process is integrated into the Automated Requisition Tool, there are no system controls that prevent a bypass from occurring.

The vast majority of bypassed requisitions were for classified service contracts. FBI contracting personnel told us that while they understood the necessity of the FBI applying C-SCRM procedures to *new* service contracts and task orders, they often intentionally bypassed requisitions for *existing* contracts because the associated companies had previously been assessed and they believed that submitting each and every subsequent requisition would be impractical, administratively burdensome, and lead to funding concerns. ASU officials told us that with the exception of incremental funding, it is essential for requisitions on existing classified service contracts (e.g., exercised option years and bridge contracts) to undergo the C-SCRM process because there may have been changes in company ownership, the contract's scope, or the company's facility clearance that occurred since ASU originally conducted its vendor threat assessment. ASU and FBI contracting personnel could benefit from enhanced communication, collaboration, and training to ensure that contracting personnel understand these requirements and identify and submit classified service requisitions that must go through the C-SCRM process. This could be facilitated through the reestablishment of a Procurement Collaboration Committee that existed before the COVID-19 pandemic, or through the creation of a C-SCRM Program Management Office, which we describe in the FBI Could Better Integrate C-SCRM Across the Organization section of this report.

Government Purchase Cards

FBI ICT purchases of $10,000 or less can be made via a government purchase card and are tracked in a system controlled by the FBI Finance Division. Unlike the Automated Requisition Tool, the government purchase card system is not directly linked into the C-SCRM module from which ASU and the SCRM Unit initiate their reviews. Instead, government purchase card holders must, prior to initiating a purchase request, enter details into a standalone C-SCRM module called "SCRM Second Entry." In the fourth quarter of FY 2020, FBI government purchase cardholders purchased approximately $30 million in goods, including ICT items.

---

[41] Such requisitions provided additional funding to existing classified service contracts. ASU officials agreed that though these are often improperly flagged for C-SCRM review and therefore characterized as bypasses, "there is no [supply chain] risk at all." The FBI bypass report did not contain sufficient detail for us to reliably identify and extract these incremental funding requisitions.

The SCRM Unit's then Unit Chief said the majority of completed C-SCRM assessments are for ICT goods purchased by FBI field offices via government purchase card and that cardholders can buy a lot of ICT items for under $10,000. This official also expressed concern that some cardholders were bypassing the C-SCRM process. The government purchase card system does not have internal controls that require cardholders to submit applicable ICT purchase information into the SCRM Second Entry portal before proceeding with the purchase. Cardholder compliance with the C-SCRM requirements is at best, mandated through guidance, such as ASU and SCRM Unit instructional documents. FBI Finance Division's purchase card policy guide did not mention C-SCRM requirements.

We analyzed a judgmental sample of 20 government purchase card requests to better quantify the frequency for which cardholders bypass the C-SCRM process. We determined that 10 of the 20 purchase requests had improperly bypassed the FBI's C-SCRM program, given that FBI officials were not able to provide procurement risk assessments for those purchase requests. FBI explained that these cardholders were often unaware of the C-SCRM requirements and stated that they had since submitted a C-SCRM request for the purchases. Notably, of the 10 bypassed purchase requests, we found that 5 were from vendors for which ASU had issued a "critical" rating and from whom SecD recommended not purchasing. Therefore, government purchase cards also appeared to bypass the C-SCRM process, but to an unknown extent, given the FBI's lack of a mechanism to monitor whether bypasses were occurring.

Overall, the FBI did not have sufficient internal controls to ensure that applicable requisitions and purchase requests were subjected to its C-SCRM program. Importantly, purchases that bypassed the FBI's C-SCRM program would not undergo the risk assessment processes described in the following section of this report. Nor would ICT goods receive OCIO-prescribed mitigation steps to address any identified risks. FBI purchases that bypass the C-SCRM processes increase the risk of compromising the FBI's IT environment and the integrity of its systems and data. We therefore recommend that the FBI enhance its policies, procedures, training and communication, and/or internal controls for the requisition and government purchase card systems to better ensure that purchasing officials understand the C-SCRM requirements and so that applicable requisitions and purchase requests undergo C-SCRM procedures, as required; and develop policies, procedures, and/or internal controls to periodically monitor FBI compliance by identifying and remedying purchases that improperly bypassed the process.[42]

Review of the FBI's C-SCRM Deliverables

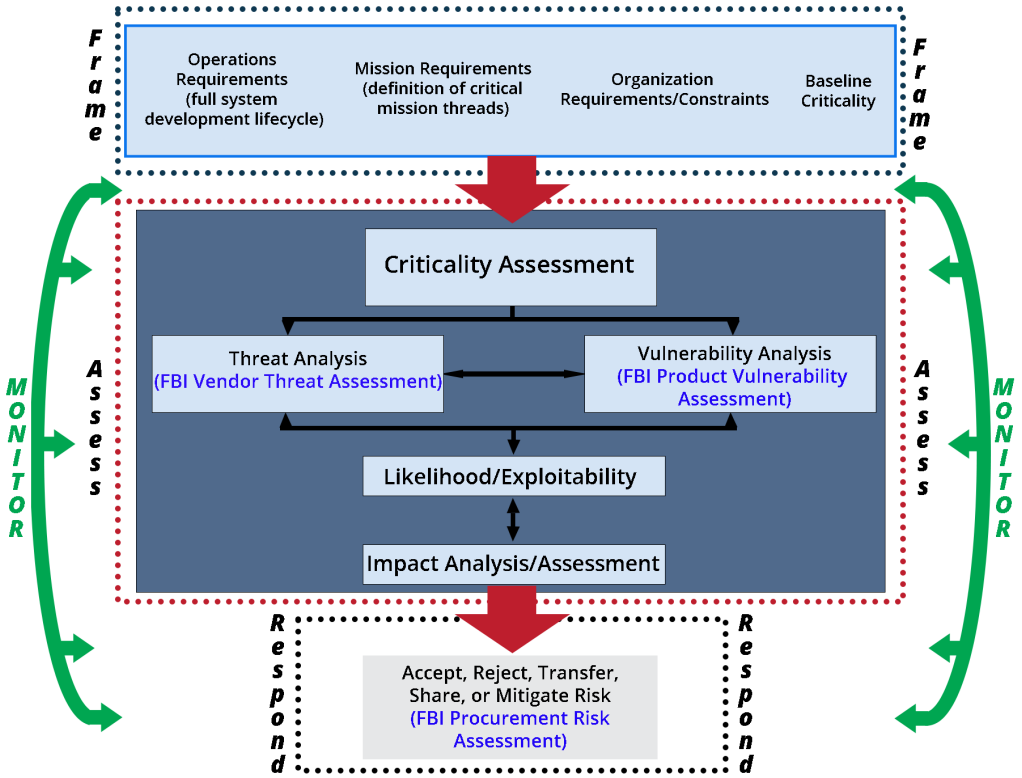
IC Directive 731 and its five standards (IC Standard 731-01, 731-02, 731-03, 731-04, and 731-05) identify the C-SCRM requirements for USIC members. IC Directive 731 is the overarching directive that requires risk assessments for mission-critical acquisitions. The IC 731 Standards provide detailed guidance on each element of the risk assessment. The supply chain risk assessment process identified in IC Directive 731, shown in Figure 3, combines four elements – threat, vulnerability, likelihood, and impact – to establish an overall risk level for the acquisition. As a member of the USIC, the FBI must apply IC Directive 731 and the

[42] In February 2022, the FBI stated that it was in the process of transitioning from the Automated Requisition Tool to its newly developed Standard Hub for Ordering and Purchasing. FBI noted that it is in the early stages of rebuilding the C-SCRM functions into this new system, including a control that requires applicable requisitions undergo the C-SCRM process. FBI expects the Standard Hub for Ordering and Purchasing to be completed by the first quarter of FY 2023.

associated standards to its mission-critical acquisitions. At the end of this process, the FBI must make a risk-based decision of whether to accept, reject, transfer, share, or mitigate the risk.

Figure 3

IC Directive 731 Supply Chain Risk Assessment Process



Source: OIG, based on a figure from IC Standard 731-02 and the National Institute of Standards and Technology, with FBI deliverables inserted in blue text.

As part of our analysis of the FBI's C-SCRM program, we examined the following four processes or deliverables to determine if they complied with IC Directive 731, its associated standards, and FBI policy: (1) criticality assessments, (2) vendor threat assessments, (3) product vulnerability assessments, and (4) procurement risk assessments.[43] We determined that the FBI has made significant progress towards modernizing and operating its C-SCRM program within the past few years. However, as summarized below, we identified several potential areas of improvement.

[43] FBI's internal C-SCRM policy is titled "*Acquisition Security Program Policy Directive 1121D,*" dated March 10, 2021.

Figure 4

Summary of FBI Compliance with IC Directive 731 and its Five Standards

USIC Criteria for C-SCRM		Type of Risk Assessment	FBI Unit Responsible	Compliance Status	Compliance Description
IC Directive 731	*Supply Chain Risk Management (2013)*	All	Acquisition Security Unit & SCRM Unit	★★☆	**Partially compliant.** The Acquisition Security Unit and the SCRM Unit are performing the required risk assessments for C-SCRM, but ASU and the SCRM Unit could improve their risk assessments to better align them with the IC 731 Standards. We also noted FBI noncompliance with other IC Directive 731 requirements, see the JMD and the FBI did not Comply with Congressional and External C-SCRM Requirements section.
Requires risk assessments (criticality assessment, threat assessment, vulnerability assessment and mitigation information) for acquisitions of mission-critical ICT products.					
IC Standard 731-01	*Supply Chain Criticality Assessments (2015)*	Criticality Assessment	SCRM Unit	★★★	**Compliant.** The SCRM Unit developed a criticality assessment for ICT products. Because the criticality workflow was newly implemented, we did not evaluate the process or the assessments that resulted from the new workflow. See the Criticality Assessments section.
Requires a criticality assessment for ICT products to determine mission-criticality by identifying the specific products to be acquired, the environment in which the items will be used, and the proposed vendors.					
IC Standard 731-02	*Supply Chain Threat Assessments (rev. 2019)*	Vendor Threat Assessment	Acquisition Security Unit	★★☆	**Partially compliant.** The Acquisition Security Unit could improve its vendor threat assessment by including the threat ratings identified in this IC Standard, ensure its assessments conform to USIC requirements for sourcing disseminated analytic products, and follow the requirements for updating the assessments. See the ASU Vendor Threat Assessments section.
Requires a threat assessment for mission-critical products that evaluates and assigns a level of threat to the integrity, trustworthiness, and authenticity of the product's supply chain, including business practices and relationships.					
IC Standard 731-03	*Supply Chain Information Sharing (2017)*	Vendor Threat Assessment & Product Vulnerability Assessment	Acquisition Security Unit & SCRM Unit	Could Not Assess	**Could Not Assess.** FBI C-SCRM personnel do not have access to the USIC repository necessary to meet the information sharing requirements. See the C-SCRM Information Sharing Requirements for USIC Members section.
Requires threat assessments and vulnerability and mitigation information be shared within a common collaborative environment (known as the C-SCRM repository).					
IC Standard 731-04	*Supply Chain Vulnerability Assessments (2019)*	Product Vulnerability Assessment	SCRM Unit	★★☆	**Partially compliant.** The SCRM Unit could improve its evaluation of ICT product vulnerabilities and assign a vulnerability rating for each vulnerability identified and include relevant information from the vendor threat assessment. See the FBI SCRM Unit's Product Vulnerability Assessments section.
Requires a vulnerability assessment that evaluates and assigns a vulnerability rating for each vulnerability and identifies known mitigations.					
IC Standard 731-05	*Supply Chain Risk Assessments (2019)*	Procurement Risk Assessment	SCRM Unit	★★☆	**Partially compliant.** The SCRM Unit could improve its procurement risk assessment to determine the likelihood of successful attacks and apply a likelihood rating; an impact analysis of the impacts of a compromise and apply an impact rating and identify an overall risk score for the procurement. See the FBI SCRM Unit's Procurement Risk Assessments section.
Requires a likelihood analysis based on the combined assessment of threat and vulnerability, assignment of a likelihood rating, an impact analysis that evaluates the effect of a compromise and the impact of mitigating and recovering from the compromise, and communication of an overall risk score for the procurement.					

Source: OIG, based on analysis of IC Directive 731 and its associated standards

Criticality Assessments

Because the IC Directive 731 supply chain risk assessment requirements only apply to acquisitions of mission-critical products, materials, and services, conducting a criticality assessment is the first step in the C-SCRM assessment process. A criticality assessment is a review to identify critical functions and components based on the potential harm caused by the probable loss, damage, or compromise of a product, material, or service to an organization's operations or mission. A criticality assessment should be conducted for all procurements to determine whether a risk assessment is required.

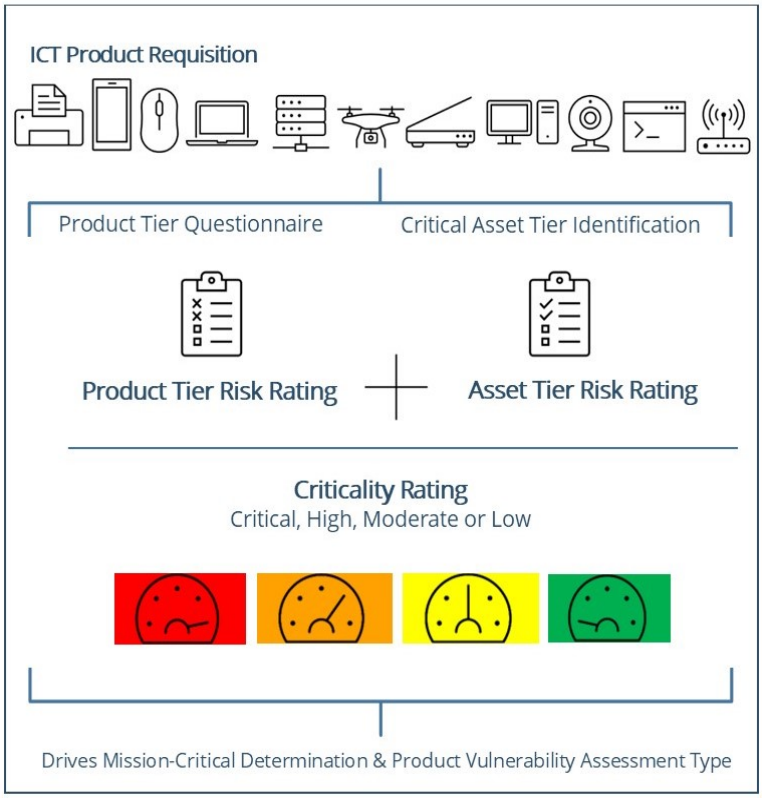
The SCRM Unit's Criticality Assessment for ICT Product Procurements & Pre-Assessed Products List

From late 2019 through 2020, the SCRM Unit performed C-SCRM assessments for almost all ICT procurements because the FBI considered them mission-critical. This resulted in a significant C-SCRM workload; in FY 2020 for instance, the FBI had approximately $2.2 billion in purchase requests that were subject to C-SCRM. FBI's broad designation of mission-criticality raised concerns that "if everything is critical, nothing is critical." The SCRM Unit recognized this challenge, noting that the FBI needed to better filter these procurements because it could not perform risk assessments for everything. To help determine which ICT products are truly mission-critical, the SCRM Unit developed a criticality assessment that it began applying to ICT requisitions submitted in October 2021.

The SCRM Unit's criticality assessment workflow results in a product tier risk rating and an asset tier risk rating for ICT products. The product tier rating uses a questionnaire to identify the level of impact on the confidentiality, integrity, and availability of FBI assets. Product responses are weighted, aggregated into a total score, and assigned a product tier rating of either critical, high, moderate, or low. The asset tier rating is based on whether an acquired product will interface with an FBI IT Critical Asset and the mission essential function impact level of that asset.[44] To determine whether the ICT product is mission-critical, the SCRM Unit

Figure 5

The SCRM Unit's Criticality Assessment for ICT Products



Source: OIG figure, based on the SCRM Unit Criticality Matrix

[44] An IT Critical Asset is any FBI IT system, application, network, or interface control that if compromised, disrupted, or destroyed would have an adverse impact to the FBI, Intelligence Community, or U.S. government operations, assets, or personnel.

combines the product tier rating and the asset tier rating to calculate a criticality rating of critical, high, moderate, or low. The SCRM Unit uses the criticality rating to drive the type of product vulnerability assessment an ICT product receives. This workflow is depicted in Figure 5. For additional discussion on the product vulnerability assessment, see the FBI SCRM Unit's Product Vulnerability Assessments section.

In addition to the criticality assessment, the SCRM Unit created a pre-assessed products list, containing hardware and software products that have previously been assessed. The SCRM Unit created this list to better manage the volume of mission-critical ICT products it must assess and emphasized that this list should not be construed as an approved products list and does not grant authority to make a purchase. Purchases of products on the list are still required to undergo the C-SCRM processes. This list helps the SCRM Unit expedite its process and identify the mission-critical products that require the highest level of assessment.

We did not review requisitions where the SCRM Unit applied its criticality assessment because it had only began applying the assessment to ICT product requisitions at the end of our audit. If implemented as described, we believe both the criticality assessment and the pre-assessed products list will help the SCRM Unit manage the large volume of requisitions for ICT products and ensure better compliance with USIC guidance. We also believe the criticality assessment will better focus the SCRM Unit's efforts on the products that are truly critical and pose the highest risks to the FBI.

Acquisition Security Unit Vendor Threat Assessments

Vendor threat assessments are Acquisition Security Unit (ASU)-conducted, research-based intelligence documents, created from open and classified sources, that assess potential threats of doing business with a company. To determine if ASU had completed vendor threat assessments (labeled "Threat Analysis" in Figure 3) in accordance with FBI and USIC requirements, we judgmentally selected a sample of 25 assessments. Our review determined that ASU generally completed vendor threat assessments in accordance with FBI guidance and IC Standard 731-02's minimum content requirements; assigned threat ratings; sufficiently detailed the basis of its determinations; queried information from several publicly available and classified sources; and typically conducted the assessments every 2 years, as required. However, we also identified four key areas of improvement.

FBI Vendor Threat Assessments Should Incorporate USIC Threat Rating Requirements

IC Standard 731-02 states that threat assessments shall evaluate and then assign a level of threat to the integrity, trustworthiness, and authenticity of the acquisition's supply chain in accordance with specific threat rating criteria, detailed in Appendix 3. ASU had not incorporated these rating definitions into its threat assessment process. Nor had ASU's vendor threat assessments framed its analysis based upon the capabilities and intent of foreign intelligence entities and adversaries, or explicitly answered the questions contained within IC Standard 731-02's Appendix B, titled "Potential Threat to U.S. National Security from this Vendor/Acquisition Item."[45] Instead, ASU rated vendors based on a threat rating tool called the Acquisition

[45] IC Standard 731-02, Appendix B contains minimum requirements for USIC elements' preparation of supply chain threat assessments and has a section titled "Potential Threat to U.S. National Security from this Vendor/Acquisition Item" that asks if vendors have a history of malicious items; if there is indication of malicious activity associated with a vendor or acquisition item, whether a foreign intelligence entity collected or attempted to acquire the acquisition item; and

Continued

Risk Directorate Threat Matrix (Threat Matrix) that was developed in 2007; however, the policy requiring use of the Threat Matrix was rescinded and replaced with IC Directive 731 in December 2013.[46] A National Counterintelligence and Security Center (NCSC) official told the OIG that their intent when developing the threat level definitions was to attain more consistent and comparable C-SCRM analytic products throughout the USIC.[47] The Threat Matrix's threat level definitions were often inconsistent with IC Standard 731-02, so that a "medium" or "high" rating under the Threat Matrix could mean something totally different than under IC Standard 731-02. Furthermore, ASU's use of the Threat Matrix generally resulted in higher ratings than would have been attained under IC Standard 731-02. JMD's C-SCRM Program Manager, who also uses Threat Matrix to complete vendor threat assessments, echoed this sentiment, noting that the Threat Matrix often results in vendors being rated "high," making it difficult to differentiate vendor risk. Because IC Standard 731-02's assessed threat level also drives a "likelihood level" and final "overall risk score," ASU's vendor threat assessment ratings would be inconsistent with and noncomparable to similar products completed by other USIC elements that followed IC Standard 731-02's threat rating criteria. This is problematic because IC Standard 731-02 strives for a common understanding, re-use, and information sharing across the USIC.

ASU officials said they continued to utilize the Threat Matrix because there was no other document that met the needs of their mission; that IC Standard 731-02 conveyed general guidelines instead of requirements; that the Threat Matrix was more objective and afforded more flexibility to rate vendors than the IC Standard 731-02 process; and that it would be laborious to create and train ASU staff on the new process. We disagree with these comments. IC Standard 731-02 does not convey its language on threat assessments as general guidelines, but as requirements.[48] ASU believed that the Threat Matrix was more objective, but that doesn't mean the information collected is more valuable. However, IC Standard 731-02's focus is narrower, as it explicitly asks USIC elements to examine foreign intelligence entities' and adversaries' capability and intent to undermine supply chains, while the Threat Matrix is significantly broader and covers many more areas. Ultimately, ASU's vendor threat assessment should not be driven by a tool whose associated policy no longer exists and was in fact superseded by IC Standard 731-02. Nevertheless, we are not suggesting that ASU eliminate use of the Threat Matrix. If ASU prefers to retain the Threat Matrix for supplementary purposes, its continued use would be acceptable, as long as it is distinct from and secondary to the actual IC Standard 731-02 requirements. Lastly, JMD's vendor threat assessments were developed and based upon the FBI's approach using the Threat Matrix. Though JMD is not a member of the USIC and therefore not subject to its directives and standards, if the FBI updates its vendor threat assessment to comply with IC Standard 731-02, while JMD retains the existing approach, the Department will have two separate and inconsistent processes, affecting comparability and shared usage. We therefore recommend that the FBI

---

whether there are indications that a foreign intelligence entity or adversary has emplaced individuals within service provider's supply chain.

[46] The Threat Matrix is a classified document. The policy that previously required use of the Threat Matrix was *Director of Central Intelligence Directive 7/6, Community Acquisition Risk Center*.

[47] NCSC is a component of the Office of the Director of National Intelligence that works with executive branch departments, agencies, and the private sector across several mission areas including supply chain risk management. NCSC developed and oversees USIC implementation of and compliance with IC Directive 731.

[48] IC Standard 731-02 states that (OIG's emphasis in bold) "the threat assessment **shall** evaluate and then characterize the level of threat to the integrity, trustworthiness, and authenticity of the acquisition item, **as defined…**" referring to the threat rating levels. IC Standard 731-02 also states that "IC Elements **shall** produce supply chain threat assessments in accordance with this Standard."

update its vendor threat assessment process to incorporate IC Standard 731-02's required threat level definitions, and that JMD adopts the FBI's revised approach to ensure intra-Department consistency.

FBI Vendor Threat Assessments Should Incorporate USIC Sourcing Requirements

IC Standard 731-02 states that vendor threat assessments shall conform to USIC sourcing requirements contained in *Intelligence Community Directive 206, Sourcing Requirements for Disseminated Analytic Products* (IC Directive 206)—see the textbox for a description of this requirement. ASU's vendor threat assessments did not generally use source reference citations, source descriptors, or source summary statements. For instance, several vendor threat assessments contained sections titled "Counterintelligence Concerns" that were completely unsourced or contained ambiguous source identifiers that would not allow efficient location and retrieval of the source. In another example, ASU summarized some pertinent information that it sourced to an FBI database, but did not include the date of issuance/publication or a source descriptor. One senior OCIO official familiar with ASU's vendor threat assessments commented that it is important that these assessments follow the ethical standards of the USIC and clearly delineate between the judgment and the facts upon which the judgment is based. This official said that detailing the credibility of the source should allow the reader to clearly understand whether the judgments are sound.

IC Directive 206: Sourcing Requirements For Disseminated Analytic Products

What is IC Directive 206?
USIC requirements for sourcing information in disseminated analytic products, to enhance the credibility and transparency of intelligence analysis, and to assist readers in making an informed assessment of the quality and scope of sources underlying the analysis.

What does IC Directive 206 require of the FBI's C-SCRM Threat Assessments?
That the FBI's vendor threat assessments include "sourcing information," such as source reference citations, source descriptors, and source summary statements. Sourcing information enables readers to readily locate and retrieve sources, to assess the age and currency of information, and assess the quality and credibility of individualized and collective sourcing.

ASU officials agreed that there is room for improvement in this area and that ASU can do a better job of sourcing, including specifying where they obtained the information. However, ASU did not believe their vendor threat assessments were subject to IC Directive 206 because they do not consider them intelligence products. They also noted that ASU personnel completing the assessments were not intelligence analysts, and therefore did not have the training that was available to FBI intelligence analysts who typically perform work in accordance with this directive. ASU's Unit Chief noted that ASU personnel had previously been prohibited from enrolling in an intelligence analyst tradecraft course because it was reserved for intelligence analysts only.

An NCSC official told us that it was not NCSC's intention that the sourcing requirements only apply to intelligence analysts, but instead to all analysts—regardless of job series—who complete the threat assessments. Furthermore, this NCSC official explained that whether the FBI's vendor threat assessment is characterized as an "analytic product" or an intelligence product is not important because its aim was to ensure that USIC elements' threat assessments meet the IC Directive 206 requirement to establish a desired standard of quality, to attain uniformity across the USIC, and to help withstand potential legal challenges on a vendor or product denial.

We believe that ASU's vendor threat assessments are not currently sourced in a manner sufficient to ensure the credibility and transparency of the FBI's intelligence analysis and to assist readers in making an informed assessment of the quality and scope of sources underlying the analysis.

FBI Should Modify its Vendor Threat Assessment Process to Better Meet its Enterprise Needs

According to ASU data, from October 2016 through September 2021, ASU completed 5,287 vendor threat assessments, of which 317 (approximately 6 percent) resulted in a SecD recommendation to deny the acquisition of ICT products from the assessed company. A SecD denial recommendation does not mean the FBI will ultimately deny purchases from the company. OCIO's Authorizing Official may authorize purchase of an ICT product from a vendor whom SecD had recommended denying, because the SCRM Unit's product vulnerability assessment determined that supply chain-related threats could be mitigated through OCIO-prescribed risk-reduction strategies.

SecD and OCIO appeared to have significantly different perceptions of the FBI's risk tolerance threshold. A SecD official explained that for ICT procurements involving ASU-issued denial recommendations, OCIO constantly accepts the IT risk and grants purchase authorization. Our analysis of the FBI's IT purchase requests reached a similar conclusion; 19 of the 25 IT purchase requests that we reviewed included vendors that had received a SecD denial recommendation. In all 19 instances, OCIO accepted the risk on these purchases.[49] While this SecD official acknowledged that OCIO has the authority to accept risk on such purchases, the frequency that it occurs was harmful to ASU morale, leaving staff questioning the value of their work, and creating personnel retention challenges. An ASU analyst may spend several days researching a company, identifying derogatory information and red flags, and documenting the results in a recommendation to avoid the vendor, only to later learn that the procurement was allowed to proceed.

A senior OCIO official did not believe the vendor threat assessments provided sufficient information for OCIO to make a full decision on any product, company, service, or device, and that the assessments could benefit from adding information on vendor cybersecurity, including whether vendors have an acceptable security posture and have been the subject of cyberattacks. OCIO officials identified three options that they believed would enhance the assessments: (1) SecD adjust the current vendor threat assessment process to better address OCIO needs; (2) OCIO share responsibility for completing the vendor threat assessments; or (3) OCIO obtains from ASU full responsibility for completing vendor threat assessments for ICT products, while ASU would retain responsibility for classified services. OCIO and SecD officials had diverse views on these options. Some officials preferred the first or second options, saying there was value in maintaining the current hybrid model, and having two separate and independent FBI components sharing C-SCRM program responsibilities. Other officials were receptive to the third option, which they believe better suited their respective missions and could resolve the issue of having C-SCRM processes divided between separate management chains.

[49] We also found that the procurement risk assessments for 7 of these 19 instances improperly stated that the company had been approved by ASU, when ASU had actually recommended denial.

ASU's Vendor Threat Assessments Should be Updated Timely

To ensure currency and accuracy, vendor threat assessments shall be reviewed at least once every 2 years for appropriate modifications to address changing conditions within the supply chain.[50] As of April 2021, ASU had 298 expired vendor threat assessments, about 28 percent of its annual workload, which on average were 513 days past expiration.[51] According to ASU's Unit Chief, ASU was unable to complete a timely update of these assessments due to a lack of staff and the volume of new requisitions requiring vendor threat assessments. Furthermore, ASU does not proactively update its vendor threat assessments immediately upon expiration but does so when ASU next receives a requisition request for ICT goods involving the company, which could be months or years after the assessment expired.[52]

To address the above matters, we recommend the FBI ensure that ASU analysts receive the training and resources necessary to fulfill IC Standard 731-02's sourcing requirements and that ASU then incorporates the IC Directive 206 sourcing procedures into its vendor threat assessment process; that ASU and the SCRM Unit modify the existing vendor threat assessment process to better align its information collection methodology, risk tolerance levels, and other attributes with the enterprise needs; and that ASU develops policies or procedures to ensure that ASU vendor threat assessments, especially those for high or critical risk vendors, are updated every 2 years, as required by IC Directive 731.

FBI SCRM Unit's Product Vulnerability Assessments

The SCRM Unit's product vulnerability assessment outlines the specific technical risk of an ICT product and the appropriate measures to reduce that risk. The SCRM Unit has adjusted and refined the applicability of its product vulnerability assessments since it assumed responsibility for this deliverable in around December 2019. For FYs 2019 and 2020, the SCRM Unit completed product vulnerability assessments for all ICT products that met one of the following criteria:

	The ICT product had wireless capabilities;
	The ICT product was open-source software; or
	The company associated with the ICT product received a "critical" rating within the Acquisition Security Unit's Vendor Threat Assessment.

[50] IC Directive 731, Section E(3).

[51] We identified the 298 expired vendor threat assessments based on a list provided by ASU. ASU's Unit Chief explained that this list may include vendors whose products are no longer used in the FBI's IT operating environment or whose staff are no longer providing classified services within the FBI. For such companies, it would not be necessary for ASU to update their vendor threat assessments. However, the FBI was unable to specify which companies from the list no longer had IT products or an employee presence within FBI space.

[52] In February 2022, the FBI said that ASU intended to enhance its internal controls to identify expiring vendor threat assessments more promptly.

In September 2020, the SCRM Unit adjusted its application of the product vulnerability assessment to focus on open-source software. In October 2021, the SCRM Unit readjusted its approach through the development of its new criticality assessment (see the Criticality Assessments section), which is applied to all ICT requisitions and results in a criticality rating that drives the type of product vulnerability assessment a product receives. The mission-criticality rating determines whether the product will receive a standard, specific, or custom product vulnerability assessment. The SCRM Unit has created standard product vulnerability assessments for 18 IT subcategories, including external storage devices, audio visual equipment, forensic devices, security appliances, wireless devices, network devices, and several others. For example, if the SCRM Unit receives an ICT requisition for a television and its criticality assessment rates the product as low or moderate, the SCRM Unit will apply the standard product vulnerability assessment for audio visual equipment to that requisition. However, if a requisition for a network device (e.g., network load balancer) is rated high or critical, the SCRM Unit will complete a specific or custom product vulnerability assessment for that requisition.

To assess the SCRM Unit's product vulnerability assessments (labeled "Vulnerability Analysis" in Figure 3), we judgmentally selected a sample of 25 FBI ICT requisitions. Because the SCRM Unit has continued to evolve its product vulnerability assessment, we judgmentally selected 13 additional assessments completed by the SCRM Unit during FY 2021 to better capture its more recent procedures. The product vulnerability assessments we reviewed were completed prior to the SCRM Unit's application of its mission-criticality assessment.

FBI SCRM Unit's Evaluation of ICT Product Vulnerabilities Could Be Improved

A product vulnerability assessment is one part of the C-SCRM risk assessment process required by IC Directive 731. Specifically, IC Standard 731-04 requires:

	Identification of vulnerabilities applicable to a product throughout its lifecycle, from design to disposal;
	Specific information on ICT products, such as whether a current vendor threat assessment exists;
	Evaluation and characterization of each vulnerability for an ICT product and its supply chain, given the efforts of foreign intelligence entities and any other adversarial attempts at compromising the ICT product;
	An assessment of the ease of exploiting a specific vulnerability by a threat actor with modest capability and mitigation information, including its method of exploitation, if there is evidence that an exploit already exists, and whether the vulnerability was previously exploited;
	Identification of relevant mitigations that could increase the difficulty of exploiting the vulnerability, implementation information for known mitigations, mitigation advice for when no known fix is available, and identification of any available alternative acquisition items without the vulnerability; and

Assigning a rating for each vulnerability using a scale of low to critical.

Our review of these requirements determined that the SCRM Unit's product vulnerability assessments generally contained information about ICT products; vulnerability information, including publicly disclosed information-security vulnerabilities and exposures; and standard mitigation actions for an ICT product or product category. However, the assessments did not include the rating the Acquisition Security Unit assigned the vendor in its vendor threat assessment, or necessary information from that assessment. Additionally, the SCRM Unit's product vulnerability assessments did not fully evaluate product vulnerabilities, including assessing the ease of exploitability by a threat actor with modest capability and mitigation information, or address the other exploitability areas, as required by IC Standard 731-04. Although the product vulnerability assessments included information on unintentional and intentional threats and threat exploitation, it was generalized for the product (e.g., insider threat, supply chain compromise, or cyber-attack) and not targeted to address a specific vulnerability and the ease of exploitability by a threat actor. Additionally, the product vulnerability assessments did not identify whether alternative products without the vulnerability were available, although we identified some recommendations from OCIO and the SCRM Unit that requesters choose a different product, known as "re-directs." However, such re-direct decisions are not documented in the product vulnerability assessment or the procurement risk assessment.

IC Standard 731-04 Supply Chain Vulnerability Assessments: Key Terms

Mitigation - The elimination or reduction of the likelihood, magnitude, or severity of exposure to risk.

Threat Actor with Modest Capability - Small, organized terrorist or criminal group, or a competent individual hacker, that can devote a few days to exploiting a product and its supply chain using well-known publicly available tactics and tools.

Vulnerability - An attribute or characteristic that may be inherent or introduced into a system's, component's, or service's design, implementation, or operation and management that could be exploited by an adversary at any stage of the acquisition lifecycle.

Vulnerability Assessment - A process of formally and systematically evaluating and documenting information on vulnerabilities that have been or could be exploited by an adversary.

Further, IC Standard 731-04 requires each evaluated vulnerability to be rated critical, high, medium, or low. The product vulnerability assessments we reviewed did not assign a rating for vulnerabilities identified for the ICT product, in line with the IC Standard 731-04 rating scale, as shown in Appendix 3. While the SCRM Unit identified mitigation recommendations in the product vulnerability assessments; most of the identified actions did not appear to address specific product vulnerabilities but were standard procedures or best practices (e.g., follow FBI policy, allow only authorized use of the product, and follow security best practices). IC Standard 731-04 defines mitigation as the "elimination or reduction of the likelihood, magnitude, or severity of exposure to risk."

NIST and USIC guidance both highlight that vulnerability assessments are an essential piece of the C-SCRM assessment process. A complete vulnerability assessment is critical to understanding which ICT product vulnerabilities may be susceptible to exploitation – a key step necessary to evaluating the likelihood of exploitation and the impact of a compromise on the organization and its mission. Therefore, we recommend the FBI improve its product vulnerability assessments for mission-critical ICT products by incorporating necessary information from the vendor threat assessments, evaluating vulnerabilities and the

ease of exploitability by a threat actor, identifying whether specific mitigations exist to address product vulnerabilities, and assigning a vulnerability rating to each vulnerability identified, to better align the product vulnerability assessment with IC Standard 731-04.

FBI SCRM Unit's Procurement Risk Assessments

The SCRM Unit's procurement risk assessment is the final step in the FBI's C-SCRM process and contains the formulization of the understood risk of a certain procurement and the associated mitigation plans. The SCRM Unit intends for it to summarize the risks from the vendor threat and product vulnerability assessments, and to document the FBI's approval or acceptance of risk for assessed ICT products. We evaluated the SCRM Unit procurement risk assessments against the requirements in IC Standard 731-05 Supply Chain Risk Assessments, focusing on the likelihood and impact analyses and identification of an overall risk score.

IC Standard 731-05 Supply Chain Risk Assessments: Key Terms

Availability - Timely and reliable access to and use of a product or its supply chain. A loss of availability is the disruption of access to or use of a product or its supply chain.

Confidentiality - The preservation of authorized restrictions on information access and disclosure, including the means for protecting personal privacy, proprietary information, and classified information. A loss of confidentiality is the unauthorized disclosure of information.

Integrity - The prevention of improper modification or destruction of a product or its supply chain and includes ensuring non-repudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of a product or its supply chain.

Likelihood Analysis – An evaluation of the likelihood that an adversary could exploit a product vulnerability and cause a compromise of a product or its supply chain (referred to as an "event"). This analysis should be based on the combined vendor threat and product vulnerability assessments, and assign a likelihood level for each vulnerability using the IC Standard 731-05 rating scale of very likely to unlikely.

Impact Analysis – Determine the impacts of a compromise and of mitigating and recovering from that compromise, and then assign an impact level for each vulnerability using the IC Standard 731-05 rating scale, shown in Appendix 3.

FBI SCRM Unit's Procurement Risk Assessments Should Include Likelihood and Impact Analyses and Communicate an Overall Risk Score

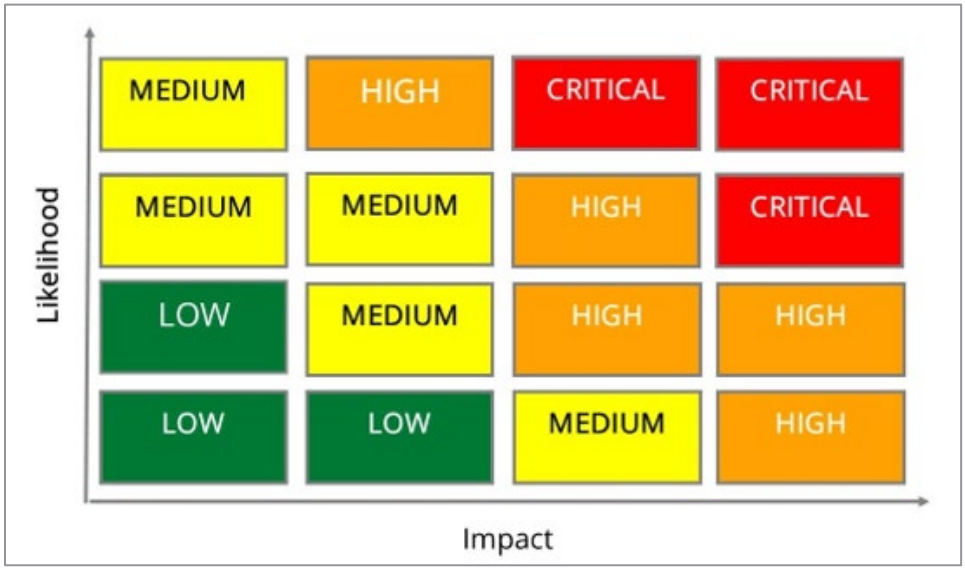
The objective of a likelihood analysis is to assess the net effect of a vulnerability, combined with threat information, to determine the likelihood of successful attacks. The SCRM Unit's procurement risk assessment did not analyze the likelihood of an event, nor did it include the information from the Acquisition Security Unit's (ASU) vendor threat assessments necessary to complete that analysis. Specifically, the SCRM Unit's procurement risk assessments only briefly referenced the vendor threat assessments' company approval or denial recommendation but did not include the actual rating assigned to the company by ASU (i.e., low, medium, high, or critical) or information on why ASU assigned that rating. Likelihood analysis also requires information from the product vulnerability assessment. Until October 2021, the SCRM Unit performed product vulnerability assessments only for ICT products that met specific criteria, as detailed above. The SCRM Unit has created a criticality assessment to better identify mission-critical items; as a result of applying this assessment, all ICT products will be evaluated for criticality and receive a product vulnerability assessment, and the criticality rating will determine the type of product vulnerability assessment completed for the product. See the Criticality Assessments section above.

An impact analysis should evaluate the effect of a loss of confidentiality, integrity, or availability on organizations, individuals, or missions as a result of successful exploitation of a vulnerability by an adversary. The SCRM Unit's procurement risk assessments did not assess the impacts of an exploitation or of mitigating and recovering from that exploitation, and did not assign an impact level. However, in multiple product vulnerability assessments for open-source software products, the SCRM Unit stated the following regarding potential impact: "*if vulnerabilities exist [for the product], the impact level of an exploitation can range from low to critical depending on the classification level and sensitivity of data being transmitted, temporarily stored, or received.*" This language was overbroad and neither conveyed whether an impact analysis was conducted, nor if an impact rating was assigned.

As discussed in the Review of the FBI's C-SCRM Deliverables section, the supply chain risk assessment process brings together four elements – threat, vulnerability, likelihood, and impact – to establish an overall risk level for a product. While the SCRM Unit views the procurement risk assessment as the final summary of the FBI C-SCRM process that documents the FBI's approval or acceptance of risk for the assessed ICT product, it does not determine or document an overall risk score for the product that is derived from the combined judgements regarding likelihood and impact. The procurement risk assessments should determine and communicate an overall risk score for the product, as directed by IC Standard 731-05. The overall risk score can be communicated using a matrix, such as the example shown in Figure 6.

Figure 6

Overall Risk Score Matrix



Source: OIG figure, based on IC Standard 731-05

We recommend the FBI improve the procurement risk assessment for mission-critical ICT products by incorporating necessary information from the vendor threat and product vulnerability assessments; complete likelihood and impact analyses for identified vulnerabilities, including assigning likelihood and impact ratings; and document an overall risk score for the procurement, to better align the procurement risk assessment with IC Standard 731-05.

FBI Should Better Document and Track OCIO Re-Direct Decisions

OCIO's Authorizing Official is delegated the responsibility to accept or deny information technology risk on behalf of the FBI. This includes denying the procurement of an ICT product based on the risk assessments performed by the Acquisition Security Unit (ASU) and the SCRM Unit as part of the FBI's C-SCRM process. The SCRM Unit's procurement risk assessment is the record that OCIO uses to document whether the Authorizing Official approves or denies the procurement of an ICT product. According to OCIO, from October 2017 to March 2021, the Authorizing Official had not denied an ICT product procurement based on the procurement risk assessment, either because OCIO found sufficient mitigation to accept the risk; or because OCIO or SecD convinced the requester to select an alternative, lower risk product, which the FBI refers to as a "re-direct." FBI had not documented or tracked ICT product procurements that were re-directed to another lower-risk product, including the alternative products that the requester purchased. IC Standard 731-04's requirements for mitigations include identifying if alternative products without vulnerabilities that cannot be mitigated are available. Further, the Department submits quarterly C-SCRM statistics to Congress, including the number of FBI ICT procurements that were re-directed due to supply chain risks.

Because the FBI does not track such re-directs to alternative products, it has only reported the number of ASU vendor threat assessments with denial recommendations. As previously explained, ASU denial recommendations are only one component of the FBI's C-SCRM process and do not represent OCIO's final decision to accept or deny the product based on the full C-SCRM assessment for the product. Because ASU denials are different from re-directs to alternative products, the FBI's current and prior reporting to Congress is inaccurate. To provide accurate numbers to Congress, OCIO would have to develop a capability to track actual re-directed ICT procurements. Lastly, the FBI could benefit from tracking its re-directed ICT procurements to periodically ensure that the highest-risk ICT items are not bypassing the C-SCRM procedures. See the section FBI's Procurements Appear to Often Bypass the C-SCRM Process Thereby Increasing Risk for further details. We therefore recommend that the FBI work with OCIO and the SCRM Unit to track and document ICT product procurement re-direct decisions in order to properly report these procurements to Congress, better improve compliance with IC Standard 731-04, and enhance the FBI's capability to ensure that high-risk products do not bypass C-SCRM processes.[53]

FBI Identification and Monitoring of Mitigation Actions Needs Improvement

A critical facet of the C-SCRM process is developing mitigation strategies to combat identified susceptibilities, vulnerabilities, and threats. IC Standard 731-04 defines mitigation as the elimination or reduction of the likelihood, magnitude, or severity of exposure to risk, and vulnerability assessments are required to identify mitigation actions for product or service vulnerabilities. The National Institute of Standards and Technology states that after organizations have identified and assessed supply chain risks, they should develop, document, and monitor performance of mitigation actions. As discussed above, the SCRM Unit's product vulnerability and procurement risk assessments are evolving. For assessments completed in 2021, we found the SCRM Unit documented mitigation actions in the product vulnerability assessment or some procurement risk assessments for ICT products. The Acquisition Security Unit (ASU) does not identify mitigation actions in its vendor threat assessment or procurement risk assessment that it

[53] In February 2022, the FBI informed us that the SCRM Unit began developing a process to track OCIO re-direct decisions.

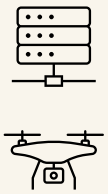
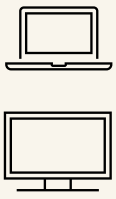
completes for classified service requisitions.[54] According to an ASU official, mitigations for classified service requisitions would be handled by the Division or Field Office Chief Security Officer and include actions such as visitor access requirements that contractor personnel are required to complete before receiving approval to work in FBI space.

For the FBI's C-SCRM program to be effective, mitigation actions need to be descriptive and actionable, and eliminate or reduce the likelihood or severity of the risk(s) with using mission-critical ICT products or services. However, identifying mitigations does not alone remove or reduce risks; users must comply with the mitigation actions to address the risks of ICT products, especially mission-critical products to prevent undue risk to the FBI and its networks. A SCRM Unit official told us they do not receive confirmation or certification from users on whether the mitigation actions the SCRM Unit identified were followed, or communication of any concerns identified through testing or inspections prior to using the product. Additionally, a SCRM Unit official could not recall whether the FBI's Operations Technology Division had determined whether a commonly referenced mitigation action requiring an inspection for hardware ICT products was applicable and had ever been performed. Accordingly, we selected nine procurement risk assessments or product vulnerability assessments completed by the SCRM Unit for various ICT products and verified whether users followed a sample of the mitigation actions identified in the assessments, as detailed in Figure 7. Overall, we found the FBI was unable to identify the status of the mitigations for some of the requisitions we tested due to personnel changes, unit reorganizations, a lack of testing capabilities, or because individuals were unfamiliar with the status of the mitigation actions.

[54] The purpose of ASU's procurement risk assessment for classified service requisitions is to document approval of the requisition and the issuance of a Department of Defense Contract Security Classification Specification (DD Form 254) to the contractor. The DD Form 254 conveys the security requirements, classification guidance, and handling procedures for classified material received or generated on a classified contract.

Figure 7

Sample of the SCRM Unit's Mitigation Actions Identified for ICT Product Requisitions

The SCRM Unit Mitigation Actions	OIG Verification of Mitigation Actions
 **Requisition of Open-Source Software Product** *Scan open-source products for malicious codes in a test environment before installing on FBI networks.*	For three requisitions, the FBI provided support that mitigation actions were taken prior to using the products; and one requisition was cancelled.
 **Requisition of a Security Product** *Vendor software or firmware updates must be tested in a test & development environment. Any identified anomalies must be reported to the applicable configuration board.*	The FBI unit did not test the product in a test environment because it did not have the equipment to do so. Instead, the FBI unit took alternative action by observing the product for issues before using it on the FBI's critical network, but the FBI unit did not notify the SCRM Unit of this alternative action or provide documentation on whether any issues with the product were identified.
 **Requisitions of Network Equipment or Drones** *Coordinate with the Operational Technology Division to determine whether an inspection was required to reduce the potential for embedded surveillance or other malicious exfiltration capabilities within the product.*	While the SCRM Unit identified this action for a requisition of network equipment, the FBI stated the action was not required due to the installation location for the equipment which was unknown when the SCRM Unit performed the risk assessment for the product. FBI stated that this mitigation action had not been taken for a requisition of drones because it had not received the drones yet.
 **Requisitions of Video Equipment or Laptop Bulk Buy** *Coordinate with the Operational Technology Division to determine whether an inspection was required to reduce the potential for embedded surveillance or other malicious exfiltration capabilities within the product.*	For a requisition of various video teleconferencing equipment for use on the FBI's main networks, the FBI did not provide evidence that any testing or inspections were performed on the products prior to use. FBI did not provide evidence that any testing or inspections of a bulk buy of laptops was performed prior to use. Additionally, this bulk buy created challenges for the FBI in its attempt to identify who was responsible for the mitigation actions and whether they were followed.

Source: OIG figure, based on FBI responses

At the beginning stages of the supply chain, suppliers or manufacturers have the opportunity to manipulate products and could engage in efforts to steal, harm, or exploit government information, systems, or equipment. Thus, the anonymity of the FBI's ICT product procurements is paramount to its defensive posture. To address this risk, the FBI's Finance and Facilities Division created a contract provision titled *Minimizing Acquisition Security Risks in Deliveries*, which became the basis for an anonymity of procurement statement that the SCRM Unit now includes in every approved procurement risk assessment. Specifically, the statement requires that orders must not identify the FBI as the addressee in shipping instructions, but instead use *United States Government*, *United States Department of Justice,* or an entity with no reference to the government; and products may not be shipped directly to any United States government location from foreign vendors.[55] We found that the Contracting Officers or other FBI personnel responsible for ICT product requisitions were generally unaware of this requirement because it was documented within the FBI's case management system, which according to FBI contracting personnel, is a system that they are not typically trained to access and use.

Further, some FBI contracting personnel noted confusion with the requirement. According to the FBI, the anonymity of procurement requirement relates to the supplier or shipper of the product(s) more than the vendor and seeks to provide an additional layer of anonymity for orders from foreign suppliers and to avoid direct shipments to the FBI from foreign locations. The FBI provided the original language for the contract provision that the Finance and Facilities Division created; we noticed that the statement the SCRM Unit inserted into the procurement risk assessment did not match the full contract provision language. While the procurement risk assessment statement required that the FBI must not be identified in shipping instructions, the requirement appeared to be applied to *any* procurement of ICT product(s) and was the responsibility of FBI contracting personnel to comply with. However, we found the contract provision language included an important distinction, identifying that the *contractor* shall ensure that orders do not mention the words *'Federal Bureau of Investigation'* or the acronym *'FBI'* in any shipping instructions provided to *the foreign entity supplier*; the addressee shall be identified as *United States Government* or *United States Department of Justice* or an entity identifier with no reference to the Government, if necessary. Thus, the anonymity of procurement statement the SCRM Unit includes in the procurement risk assessment is misrepresenting the actual requirement and led to confusion of FBI contracting personnel about the requirement. We believe updating the anonymity of procurement statement in the procurement risk assessments to correctly reflect the contract provision language will help resolve confusion about the requirement. In addition, ensuring that FBI contracting personnel can access the procurement risk assessments will help contracting personnel understand and improve compliance with the requirement.

Lastly, the SCRM Unit stated that continuous monitoring, via use of technological applications to stay apprised of dynamic changes in the information technology procurement environment, is one of its top priorities. For FY 2021, OCIO and the SCRM Unit's goal was to develop a process to automate the continuous monitoring of risks outlined in the procurement risk assessments. The SCRM Unit began the search for a continuous monitoring tool in early FY 2021; however, before a contract could be awarded, the FBI diverted funds for this initiative elsewhere. A SCRM Unit official told us there was not a specific reason for the diversion of funds but noted that the SCRM Unit is planning to resume its efforts for a continuous

[55] The statement noted that this requirement was not intended to transform the requisition into a covert procurement; but the requirement is an overt action with special shipping instructions.

monitoring tool in early 2022. As a result, the FBI does not have a process or procedures in place to monitor user compliance to ensure they follow the mitigation requirements actions.

ICT procurements require identification and monitoring of mitigation actions to address product risks, especially for mission-critical products and services. We believe it is especially critical that mitigation actions for multi-product or bulk buy ICT procurements are monitored for compliance because of the increased risk from the amount of new equipment connected to FBI networks or the number of FBI personnel using the equipment. Thus, we recommend the FBI ensure mitigation actions for ICT products, especially mission-critical ICT products or services, are descriptive, actionable, and tailored to the user environment and operational contexts (including its anonymity of procurement statement); and work with OCIO and the SCRM Unit to create and resource a program that continuously monitors C-SCRM risks across the FBI, ensures that users understand and follow C-SCRM mitigations identified in the product vulnerability and procurement risk assessments, and develops procedures to periodically monitor and assess user compliance with its C-SCRM mitigation actions.

FBI Could Better Integrate C-SCRM Across the Organization

Managing cyber supply chain risk is a complex undertaking that requires a coordinated interdisciplinary approach. One of the National Institute of Standards and Technology's (NIST) key C-SCRM practices is to integrate and align C-SCRM across an organization. Such internal alignment facilitates the efficiency and effectiveness of delivering products and services while appropriately managing C-SCRM risks.

FBI's C-SCRM program is not limited to SecD and OCIO. It requires a coordinated team approach that incorporates or has a nexus to several other FBI divisions and offices. For instance, FBI Finance Division oversees the government purchase card program, and its Contracting Officers submit information on manufacturers, developers, resellers and products necessary for the C-SCRM process to commence. The FBI's Operational Technology Division maintains unique insights on supply chain risk. FBI investigative and intelligence divisions supply information that is incorporated into the Acquisition Security Unit's vendor threat assessments; requesting divisions are responsible for ensuring that ICT is deployed in accordance with OCIO's mitigation strategies; and other FBI components that have roles that are important to the C-SCRM program. The challenge is synthesizing the efforts of all relevant divisions and offices into a comprehensive C-SCRM program. FBI did not maintain an enterprise C-SCRM strategy or mechanism that consolidates, manages, and institutionalizes these efforts; and that establishes FBI-wide accountability for the execution of C-SCRM activities.[56]

[56] FBI's primary C-SCRM program policy is an FBI Acquisition Security Program Policy Directive, managed by the FBI's Security Division, which details roles and responsibilities for SecD, OCIO, Contracting Officers, and Contracting Officer's Representatives.

NIST highlights the use of a central Program Management Office (PMO) as one potential model for concentrating and assigning C-SCRM activities and responsibilities across an organization. A C-SCRM PMO typically consists of subject matter experts who help drive the C-SCRM strategy and implementation across the organization and its mission and processes. Both FBI and NCSC officials emphasized that for a C-SCRM PMO to be effective, it must have executive level commitment and accountability.

Foundational C-SCRM Practice: Program Management Office

Another NIST foundational C-SCRM practice is to establish a core, dedicated multi-disciplinary Program Management Office (PMO) to drive C-SCRM activities and serve as a fulcrum for coordinated, C-SCRM-oriented services and guidance throughout the enterprise. Such an operating model can facilitate concentrating and assigning responsibilities throughout the enterprise and offers a centralized hub for information sharing, tools, training, and awareness.

Additionally, NCSC told us that the greatest contributor to a successful C-SCRM program is executive-level commitment. A C-SCRM PMO led by an accountable FBI senior executive could help ensure that the FBI's C-SCRM strategy and implementation efforts are driven across the enterprise.

We spoke with officials at another U.S. Intelligence Community entity about its C-SCRM program and learned it was developing a PMO to better connect and align its program participants. Creating a C-SCRM PMO is one way the FBI could achieve better integration of its program across the FBI by ensuring that its program encompasses all stakeholders. It could help ensure that procurement officials receive training and are aware of the C-SCRM requirements so that they do not improperly bypass the C-SCRM process; that ICT purchasers and system owners are accountable for completing the OCIO-prescribed mitigating actions; and provide a venue to coordinate and resolve challenging matters, such as modifying the vendor threat assessment process to better meet enterprise needs.[57] An additional benefit of a C-SCRM PMO is that it can coordinate interagency C-SCRM information-sharing across the supply chain and across the organization to better inform its program. An FBI C-SCRM PMO would not require establishment of a new FBI structure. An FBI senior official suggested that such a function could reside within OCIO, with the Chief Information Officer serving as the accountable executive who assigns C-SCRM responsibilities throughout the enterprise, and monitors and evaluates their completion. However, this official noted that additional OCIO resources would be needed to establish and sustain a C-SCRM PMO.

We recommend that the FBI better integrate its C-SCRM program across the enterprise and leverage other FBI units that help inform and apply the required processes and risk decisions, such as through the use of a

[57] While the establishment of a PMO could significantly enhance FBI awareness of C-SCRM requirements, the FBI had taken steps to address this matter via training. According to an FBI official, in late 2021 the FBI developed and began offering C-SCRM training courses to educate financial managers, special agents, government purchase card holders, and other officials on the purpose and importance of C-SCRM, including supply chain risks and the relevant requirements; IT products subject to C-SCRM; and how to submit and track C-SCRM requests.

Program Management Office or similar operating model that is led by an accountable FBI executive-level official.[58]

Other JMD and FBI Noncompliance and Areas of Improvement

We found additional instances where both Justice Management Division (JMD) and the FBI did not comply with Congressional and other external C-SCRM requirements that we believe should be addressed promptly. We also believe that both components should take steps to improve information sharing within DOJ and with external partners.

JMD and the FBI did not Comply with Congressional and External C-SCRM Requirements

From FYs 2014 through 2021, the Department's annual congressional appropriations language required the Department conduct C-SCRM assessments for new FISMA reportable IT systems that the Department designated high- or moderate-impact. JMD incorporated this requirement into JMD's C-SCRM policy in 2014. According to JMD records, from October 2016 through March 2021, non-FBI Department components acquired 47 such systems, consisting of 36 moderate- and 11 high-impact. However, JMD could not provide evidence that it had conducted C-SCRM assessments for 46 of these 47 systems, as required. The C-SCRM Program Manager acknowledged that this was a compliance gap and said JMD lacked a process to identify new high- or moderate-impact information systems that required C-SCRM prior to acquisition. This official explained that JMD may have at best, incidentally applied C-SCRM procedures to some of the vendors associated with these information systems during its assessments of purchases for national security systems or foreign-owned IT. The C-SCRM Program Manager believed this matter could be addressed by updating the Department's information system inventory management tool to flag applicable systems when added to the inventory.[59] Additionally, JMD had not been reporting C-SCRM statistics to the OIG, as required by Congress since FY 2016.

FBI was also subject to this congressional requirement and from October 2016 through March 2021 had added 37 systems to its security and privacy assessment and authorization management tool, consisting of 17 moderate- and 20 high-impact systems. To assess FBI compliance with the requirement, we judgmentally selected a sample of five high- or moderate-impact information systems. FBI officials were unable to provide evidence that any of these five systems underwent C-SCRM review. OCIO told us that FBI officials responsible for system development had not disclosed to them the acquisition or development of these five systems so that OCIO could conduct a C-SCRM assessment. This likely occurred because the FBI did not have policies or procedures stipulating that new information systems undergo the C-SCRM process. OCIO officials noted however, that while they did not apply a C-SCRM assessment to the five finished information systems, that does not mean that OCIO had not assessed the individual components (software and hardware) that comprised these systems. Ultimately, both JMD and the FBI need to establish guidance and procedures to comply with this longstanding congressional requirement.

---

[58] In February 2022, the FBI stated that its SCRM Unit was developing an enterprise-wide C-SCRM plan that includes policy requirements, processes and workflows, and personnel roles and responsibilities.

[59] JMD's information system inventory management tool is referred to as the Cyber Security Assessment and Management, or CSAM.

During the course of our review, we also determined that JMD and the FBI had not complied with certain external C-SCRM requirements. First, both JMD and the FBI recognize the Committee on National Security Systems Directive 505, *Supply Chain Risk Management* (CNSS Directive 505) as a governing authority for operating their respective C-SCRM programs. CNSS Directive 505 provides requirements for the U.S. government to implement and sustain C-SCRM capabilities for national security systems. While we did not conduct a detailed assessment of Department compliance with CNSS Directive 505, we examined one requirement that U.S. government departments and agencies report on progress and effectiveness of their organization's capabilities to CNSS annually, at a minimum. We determined that neither JMD nor the FBI had submitted reports on the progress and effectiveness of their organization's C-SCRM capabilities to CNSS, as required. Both JMD and FBI officials agreed that their noncompliance was inadvertent. JMD's C-SCRM Program Manager noted that CNSS had never contacted the Department to request it and that CNSS's supply chain working group was no longer active.

We recommend that JMD and the FBI establish policies, procedures, and internal controls that ensure they follow Congressional requirements to apply C-SCRM procedures to new FISMA reportable IT systems designated high- or moderate-impact and report C-SCRM statistics to the OIG. FBI and JMD should also contact CNSS to determine if submission of an annual report on the progress and effectiveness of their C-SCRM capabilities remains an active requirement, and if so, establish policies and procedures to ensure that they submit—either separately or jointly—these reports to CNSS annually, in accordance with CNSS Directive 505.

In addition, as previously noted, IC Directive 731 defines C-SCRM requirements for the USIC. FBI's C-SCRM program applies the IC Directive 731 criteria for risk assessments to all mission-critical items purchased throughout the FBI. However, the FBI had not met all IC Directive 731 requirements. Specifically, IC Directive 731 requires USIC elements conduct evaluations of, and certify to the Assistant Director of National Intelligence for Acquisition, Technology, and Facilities the integrity of their organization's supply chain processes every 2 years. FBI had not submitted a certification of its program to the Assistant Director of National Intelligence for Acquisition, Technology, and Facilities. FBI informed us that SecD was coordinating with OCIO regarding future plans for evaluation and certification of the FBI's supply chain process. We recommend that the FBI establish policies and procedures to evaluate, certify, and submit reports to the Assistant Director of National Intelligence for Acquisition, Technology, and Facilities on the integrity of its organizational supply chain processes every 2 years, in accordance with IC Directive 731.

The Department Should Enhance its C-SCRM Information Sharing Efforts

Federal agencies are continuously exposed to risk originating from their supply chains. According to the National Institute of Standards and Technology (NIST), agencies should build information sharing processes and activities into their C-SCRM programs to aid in identifying, assessing, monitoring, and responding to cyber supply chain risks. An effective information sharing process can help agencies access information critical to understanding and mitigating cyber supply chain risks to help protect government-wide operations.

As the SolarWinds compromise has shown, cyber supply chain threats continue to increase in complexity, highlighting the need for a government-wide C-SCRM information sharing effort. A whole of government approach could leverage the collective knowledge, experience, and capabilities of agencies to gain a more complete understanding of the threats that agencies may face. Both JMD and FBI officials have commented on the importance of information sharing inside and outside the Department. Within the Department, the FBI shares its vendor threat assessments with JMD's C-SCRM Program Manager. There could be additional value in the FBI sharing its other work products and tools with JMD, including its product vulnerability assessments, procurement risk assessments (which include mitigation strategies), and its continuous monitoring efforts. Additionally, the DEA's Office of National Security Intelligence has recently begun developing its C-SCRM program to comply with IC Directive 731 and could similarly benefit from such information sharing.

NIST Critical Success Factor: Supply Chain Information Sharing

NIST states that an effective information sharing process helps to ensure enterprises can gain access to information critical to understanding and mitigation cybersecurity risk in the supply chain, and also share relevant information to others that may benefit from or require awareness of these risks. NIST's key practices for establishing and participating in supply chain risk information sharing relationships include:

- Establishing information sharing goals and objectives, specifying the scope of information sharing, and establishing information sharing rules;
- Using secure, automated workflows to publish, consume, analyze, and act upon supply chain risk information;
- Participating in information sharing efforts; and
- Proactively establishing supply chain risk information sharing agreements.

DEA officials also told us that several years ago, the Department hosted quarterly briefings that focused on C-SCRM topics such as threats to classified systems. DEA officials said these briefings were very helpful to understand supply chain risks but did not believe such a briefing has occurred since 2016. JMD and the FBI maintain unique knowledge of Department's supply chain risks and threats; developing a means to periodically share this information could greatly benefit other Department components.

There are also two on-going government-wide efforts to enhance C-SCRM information sharing. One relates specifically to USIC members which we detail in the following section. The second applies to agencies across the federal government and began with the 2018 establishment of the Federal Acquisition Security Council, an interagency council with representatives across the federal government including from the Department

and the FBI.[60] FBI's Acting Chief Information Officer explained that more connectivity and information sharing with its external partners is critical to the FBI's C-SCRM program, and that the FBI was considering establishing a memorandum of understanding with the Department of Defense in order to share information and best practices. FBI's Acting Chief Information Officer also noted that the FBI does not have a formal relationship with the National Security Agency (NSA), but given the work that NSA is doing related to C-SCRM, the FBI could consider establishing a similar agreement with NSA.[61]

Government-wide information sharing efforts through the Federal Acquisition Security Council remains ongoing and an information sharing structure has not yet been developed. However, in the interim, we believe there are opportunities for JMD and the FBI to establish relationships throughout the government to promote sharing C-SCRM information. These efforts will also prepare JMD and the FBI to share information efficiently and effectively once the Federal Acquisition Security Council establishes an information sharing mechanism. Therefore, we recommend that JMD and the FBI assess how it can better share C-SCRM information within the Department and identify opportunities to bolster C-SCRM information sharing with other federal agencies.

C-SCRM Information Sharing Requirements for USIC Members

IC Directive 731 requires USIC elements share C-SCRM threat assessments, including vulnerability and mitigation information within a C-SCRM repository that was to be developed by the Office of the Director of National Intelligence (ODNI).[62] An official from the National Counterintelligence and Security Center's (NCSC) Supply Chain and Cyber Directorate told OIG that the C-SCRM repository exists, that it is limited to USIC personnel with C-SCRM responsibilities, and that it is accessible upon completion of an NCSC-offered training course on IC Directive 731 that is anticipated to become available near the end of FY 2022.[63] An FBI official told us that use of this repository could be beneficial and help supplement their C-SCRM work. JMD's C-SCRM Program Manager agreed, stating that JMD could benefit from enhanced information sharing, such as accessing additional Intelligence Community analysis and reports. We encourage the FBI, JMD, and DEA/ONSI to attend NCSC's IC Directive 731 training, when made available, and obtain access to and begin contributing their C-SCRM risk assessments to ODNI's C-SCRM repository in accordance with IC Directive 731.

---

[60] The Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act (SECURE Technology Act) of 2018.

[61] As part of the FBI Director's Priority Initiative on digital risk, senior FBI officials suggested benchmarking the FBI's C-SCRM program against other federal agencies and noted that they considered the National Security Agency (NSA) to be the FBI's measuring stick, and that they should leverage NSA efforts. The Operational Technology Division also suggested the FBI better understand the NSA's C-SCRM program.

[62] The C-SCRM repository was to be located within the Library of National Intelligence or other designated system. The Library of National Intelligence is ODNI's repository of finished intelligence that is designed to enable discovery of information by all authorized users.

[63] While JMD is not a member of the USIC, NCSC informed us that it could gain access to ODNI's repository (upon completion of the mandatory training) because it conducts work on behalf of the Drug Enforcement Administration, which does contain a USIC element.

Finally, the National Defense Authorization Act for FY 2020 required the Director of National Intelligence to establish a Supply Chain and Counterintelligence Risk Management Task Force (Task Force).[64] The Task Force, chaired by the Director of the National Counterintelligence and Security Center, is responsible for ensuring that USIC counterintelligence information sharing is standardized, to provide actionable information to federal acquisition professionals. The Task Force also intends to reinforce IC Directive 731 standards for protecting supply chain information while sharing responsibly, support the previously described Federal Acquisition Security Council information sharing needs, and attain a unified voice on threats to the supply chain. The law also requires membership from a representative of the FBI. An NCSC official told us that it is important that Task Force participants select as their representative a senior executive who can speak on behalf of and relay information back to their organization's C-SCRM program. According to the FBI, while an official from its Counterintelligence Division had been regularly attending Task Force meetings, OCIO had not participated in about a year, and the OCIO representative had since departed the FBI and a successor had not been designated. The NCSC official said that better engagement from the FBI's OCIO would benefit the Task Force. Therefore, we believe that OCIO should designate a senior executive official from the OCIO to act as its representative and be a more active participant on this mandatory Task Force.

We recommend that the FBI designate a senior official from the OCIO as its representative for, and who actively participates on, the Supply Chain and Counterintelligence Risk Management Task Force.

[64] 50 U.S.C. § 3370(b).

Conclusion and Recommendations

JMD lacked the personnel resources necessary to effectively manage the existing C-SCRM program. We believe it was unrealistic for a single JMD employee to operate and maintain a comprehensive program that covers all non-FBI Department components. This lack of resources dedicated to the Department's C-SCRM program resulted in gaps in its ability to identify, assess, mitigate, and respond to supply chain risk throughout the information technology lifecycle. Most significantly, by not properly monitoring its C-SCRM program to ensure all components, including JMD, identified all applicable ICT purchases and submitted those requests to JMD to perform a C-SCRM assessment, the Department elevated the risk of introducing products or services into its IT environment that could compromise the integrity of its systems and data. Further, because JMD has not re-assessed the Department's systems for supply chain risk or updated its C-SCRM guidance in over 7 years, it has limited the Department's ability to adapt to evolving threats and to be responsive to organizational changes. Without enhancements to JMD's C-SCRM assessments, which are necessary to ensure each product is examined to identify vulnerabilities and estimate the likelihood and impact of an event, JMD's risk assessments and the resulting mitigation controls will continue to include gaps. In addition, JMD's existing risk mitigation actions are insufficient, and JMD has not established internal controls to monitor whether Department components follow mitigating actions stipulated within JMD's risk determination letter after proceeding with assessed IT acquisitions. We also determined that the DEA's Office of National Security Intelligence, a member of the U.S. Intelligence Community, had not established a supply chain risk management program as required by an Intelligence Community directive.

Further, while the FBI has made progress towards modernizing its C-SCRM program, it needs to improve its ability to identify, assess, mitigate, and respond to supply chain risk throughout the information technology lifecycle. Hundreds of millions of dollars in ICT goods and classified services may have improperly bypassed the FBI's C-SCRM process between October 2017 and May 2021 and, as it relates to the FBI's risk assessments, we found that key C-SCRM deliverables were not compliant with IC Directive 731, which requires each USIC element to conduct risk assessments for mission-critical acquisitions and make risk-based decisions whether to accept, reject, transfer, share, or mitigate the risk. Although the FBI identified some mitigation actions in its assessments, they were not descriptive, actionable, or tailored to the user environment and operational contexts. As of November 2021, like JMD, the FBI did not have a process or procedures in place to monitor user compliance with the mitigation requirements. FBI would benefit from better integrating C-SCRM across the organization, such as through the establishment of a Program Management Office.

Lastly, the FBI and JMD C-SCRM programs should comply with congressional and external C-SCRM requirements and should improve their information sharing efforts within the Department, with USIC members, and government-wide.

We recommend that JMD:

1. Coordinate with the BOP and FPI, EOUSA, JMD, NSD, and USMS, and other Department components that are subject to JMD's C-SCRM requirements and whose compliance statuses are unknown, to ensure they maintain or develop the procedures and controls necessary to comply with JMD's C-SCRM requirements; incorporate into its C-SCRM program steps to monitor and verify Department compliance with its guidance through periodic outreach, communication, and the establishment of

internal controls; and enhance Department awareness of its C-SCRM program, such as through training.

2. Ensure that its C-SCRM strategy consolidates the existing requirements, including for wireless communications platforms; is refreshed periodically to reflect the latest requirements, standards, and best practices; includes a periodic re-assessment of the Department systems that are most vulnerable or that would cause the greatest organizational impact if compromised; and includes processes that better promote transparency and communication of C-SCRM results to Department components.

3. Update its C-SCRM risk assessment methodology to assess vulnerabilities, likelihood, and impact, in accordance with NIST 800-161, Revision 1 and CNSS Directive 505; and that its risk assessment also be applied to resellers, particularly those handling IT goods.

4. Develop policies and procedures that enable it to establish viable mitigation options that are descriptive, actionable, and tailored to the user environment and operational contexts, to be included in risk determination letters as needed; and that it establishes internal controls to monitor Department fulfillment of the mitigating actions.

We recommend that the DEA:

5. Establish policies and procedures to ensure ONSI compliance with Intelligence Community Directive 731 and its associated standards.

We recommend that the FBI:

6. Enhance its policies, procedures, training and communication, and/or internal controls for the requisition and government purchase card systems to better ensure that purchasing officials understand the C-SCRM requirements and so that applicable requisitions and purchase requests undergo C-SCRM procedures, as required; and develop policies, procedures, and/or internal controls to periodically monitor FBI compliance by identifying and remedying purchases that improperly bypassed the process.

7. Ensure that Acquisition Security Unit analysts receive the training and resources necessary to fulfill IC Standard 731-02's sourcing requirements and that ASU then incorporates the IC Directive 206 sourcing procedures into its vendor threat assessment process; that ASU and the SCRM Unit modify the existing vendor threat assessment process to better align its information collection methodology, risk tolerance levels, and other attributes with the enterprise needs; and that ASU develops policies or procedures to ensure that ASU vendor threat assessments, especially those for high or critical risk vendors, are updated every 2 years, as required by IC Directive 731.

8. Improve the product vulnerability assessments for mission-critical ICT products by incorporating necessary information from the vendor threat assessments, evaluating vulnerabilities and the ease of exploitability by a threat actor, identifying whether specific mitigations exist to address product

vulnerabilities, and assigning a vulnerability rating to each vulnerability identified, to better align the product vulnerability assessment with IC Standard 731-04.

9. Improve the procurement risk assessment for mission-critical ICT products by incorporating necessary information from the vendor threat and product vulnerability assessments; complete likelihood and impact analyses for identified vulnerabilities, including assigning likelihood and impact ratings; and document an overall risk score for the procurement, to better align the procurement risk assessment with IC Standard 731-05.

10. Work with OCIO and the SCRM Unit to track and document ICT product procurement re-direct decisions in order to properly report these procurements to Congress, better improve compliance with IC Standard 731-04, and enhance the FBI's capability to ensure that high-risk products do not bypass C-SCRM processes.

11. Ensure mitigation actions for ICT products, especially mission-critical ICT products or services, are descriptive, actionable, and tailored to the user environment and operational contexts (including its anonymity of procurement statement); and work with OCIO and the SCRM Unit to create and resource a continuous monitoring program that monitors C-SCRM risks across the FBI, ensures that users understand and follow C-SCRM mitigations identified in the product vulnerability and procurement risk assessments, and develops procedures to periodically monitor and assess user compliance with its C-SCRM mitigation actions.

12. Better integrate its C-SCRM program across the enterprise and leverage other FBI units that help inform and apply the required processes and risk decisions, such as through the use of a Program Management Office or similar operating model that is led by an accountable FBI executive-level official.

13. Establish policies and procedures to evaluate, certify, and submit reports to the Assistant Director of National Intelligence for Acquisition, Technology, and Facilities on the integrity of its organizational supply chain processes every 2 years, in accordance with IC Directive 731.

14. Designate a senior official from the OCIO as its representative for, and who actively participates on, the Supply Chain and Counterintelligence Risk Management Task Force.

We recommend that JMD and the FBI:

15. Ensure that ASU updates its vendor threat assessment process to incorporate IC Standard 731-02's required threat level definitions, and that JMD adopts the FBI's revised approach to ensure intra-Department consistency.

16. Establish policies, procedures, and internal controls that ensure they follow Congressional requirements to apply C-SCRM procedures to new FISMA reportable IT systems designated high- or moderate-impact and report C-SCRM statistics to the OIG. FBI and JMD should also contact CNSS to determine if submission of an annual report on the progress and effectiveness of their C-SCRM

capabilities remains an active requirement, and if so, establish policies and procedures to ensure that they submit—either separately or jointly—these reports to CNSS annually, in accordance with CNSS Directive 505.

17. Assess how it can better share C-SCRM information within the Department and identify opportunities to bolster C-SCRM information sharing with other federal agencies.

APPENDIX 1: Objective, Scope, and Methodology

Objective

The objective of this audit was to determine the extent to which the Department, through JMD and the FBI, implemented an organizational supply chain risk management program that identifies, assesses, mitigates, and responds to supply chain risk throughout the information technology lifecycle.

Scope and Methodology

Our audit generally covered, but was not limited to, JMD's and the FBI's cyber supply chain risk management (C-SCRM) activities from October 2016 through January 2022. To accomplish our objective, we reviewed and assessed JMD and FBI compliance with agency and Department-level policies and procedures, and with external requirements such as from Congress, the National Institute of Standards and Technology, the Office of the Director of National Intelligence, and the Committee on National Security Systems. We evaluated JMD's and the FBI's C-SCRM programs to determine if they identified, assessed, mitigated, and responded to supply chain risk throughout the IT lifecycle. However, our audit did not include a review of the disposal segment of the IT lifecycle.

The Department has two different C-SCRM programs—one operated by and focused on the FBI; and a second operated by JMD and focused on all other non-FBI Department components. To determine if the Department was following JMD's C-SCRM requirements, we selected several Department components based on their organizational mission, amount of annual IT spending, and JMD assessment data. Specifically, we interviewed officials and analyzed information and data from the Bureau of Alcohol, Tobacco, Firearms, and Explosives; Drug Enforcement Administration; Executive Office for U.S. Attorneys; Federal Bureau of Prisons; JMD; National Security Division; and U.S. Marshals Service.[65] We examined whether each of these components acquired IT items that were subject to JMD's C-SCRM program. If so, we then assessed whether they had policies or procedures to identify and submit applicable requests to JMD's Cybersecurity Services Staff (CSS) and determined whether these components had been consistently submitting such requests. We also solicited their feedback on JMD's C-SCRM program, including whether its guidance was clear, the deliverables useful, and the overall program valuable. Additionally, we examined JMD's monitoring and oversight of Department compliance with its C-SCRM program; assessed its C-SCRM policies and procedures; reviewed its C-SCRM deliverables, including its vendor threat assessments and risk determination letters; and efforts in the area of building C-SCRM program awareness.

For the FBI, we examined whether its C-SCRM program was operated in accordance with FBI and external requirements, with an emphasis on compliance with Intelligence Community Directive 731 – Supply Chain Risk Management, dated December 2013, and its associated Intelligence Community Standards (collectively referred to as "IC Directive 731"). FBI, as a member of the U.S. Intelligence Community, is governed by IC Directive 731 procedures. OIG examined the FBI's key C-SCRM processes and deliverables including its criticality analysis, vendor threat assessments, product vulnerability assessments, and procurement risk

[65] Though the Office of the Inspector General (OIG) is also subject to JMD's C-SCRM requirements, we excluded the OIG from our audit because Generally Accepted Government Auditing Standards require auditors decline to perform work where impairments to independence can affect, or be perceived to affect, the independence of the audit organization.

assessments. We also analyzed FBI IT acquisition data to determine whether FBI procurement officials were improperly bypassing C-SCRM requirements. Next, we examined whether the FBI maintained a coordinated, enterprise approach to C-SCRM and complied with external C-SCRM requirements, including on information-sharing. Our review also broadly assessed DEA compliance with IC Directive 731, given that its Office of National Security Intelligence is also a member of the U.S. Intelligence Community.

We conducted our audit work remotely and interviewed dozens of Department officials from the FBI, JMD, and the aforementioned Department components. We also spoke with officials outside of the Department, including from the National Counterintelligence and Security Center, the National Security Agency, the Department of Homeland Security, and the Intelligence Community OIG.

Statement on Compliance with Generally Accepted Government Auditing Standards

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Internal Controls

In this audit, we performed testing of internal controls significant within the context of our audit objective. We did not evaluate the internal controls of the Department to provide assurance on its internal control structure as a whole. Department management is responsible for the establishment and maintenance of internal controls in accordance with OMB Circular A-123. Because we do not express an opinion on the Department's internal control structure as a whole, we offer this statement solely for the information and use of the Department.[66]

As noted in the Audit Results section of this report, we identified deficiencies in JMD's and the FBI's internal controls that are significant within the context of the audit objective and, based upon the audit work performed, that we believe may adversely affect their ability to achieve their C-SCRM objectives. Specifically, we found that JMD's primary C-SCRM guidance (i.e., Procurement Guidance 14-03) did not include any monitoring and oversight provisions and JMD had not taken steps to ensure Department components were compliant with its requirements. In the absence of such oversight, we found that several Department components had not been submitting applicable IT purchases for a C-SCRM review in accordance with JMD's requirements. For the FBI, we determined that it did not have sufficient internal controls to ensure that applicable requisitions and purchase requests were subjected to its C-SCRM program, resulting in acquisitions improperly bypassing the process altogether.

Compliance with Laws and Regulations

In this audit we also tested, as appropriate given our audit objective and scope—records, procedures, and practices—to obtain reasonable assurance that the Department's management complied with federal laws and regulations for which noncompliance, in our judgment, could have a material effect on the results of

[66] This restriction is not intended to limit the distribution of this report, which is a matter of public record.

our audit. Our audit included examining, on a test basis, the Department's compliance with the following laws that could have a material effect on the Department's operations:

- Consolidated Appropriations Act language from FYs 2012 – 2021 (Pub L. Nos. 112-55, 113-6, 113-76, 113-235, 114-113, 115-31, 115-141, 116-6, 116-93, and 116-260)

- Public Law 115-390, Title II, Federal Acquisition Supply Chain Security Act of 2018

This testing included interviewing auditee personnel and evaluating C-SCRM assessment data. Based on this testing, we determined that JMD and the FBI had not established internal controls that would enable them to apply C-SCRM procedures to new FISMA reportable IT systems that the Department designated high- or moderate-impact, nor had it been reporting its C-SCRM statistics to the OIG, both as directed by Congress.

Sample-Based Testing

To accomplish our audit objective, we performed sample-based testing to: (1) evaluate JMD's and the FBI's C-SCRM deliverables, (2) assess Department compliance with JMD's C-SCRM requirements, and (3) determine if FBI requisitions and purchase requests were bypassing the FBI's C-SCRM program. First, to evaluate JMD's and the FBI's C-SCRM efforts, we employed a judgmental sampling design to select 25 deliverables for each component, based on the date, product type, and resulting assessment score. Second, to assess Department compliance with JMD's C-SCRM requirements, we selected seven Department components based upon a combination of their organizational mission, amount of annual IT spending, and JMD's assessment data. Third, to determine if FBI requisitions and purchase requests were bypassing the FBI's C-SCRM program, we selected a sample of 20 requisitions included in the FBI's bypass report and 20 government purchase card requests. These sampled items were selected based on date, product type, and associated assessment data. In all three instances, these non-statistical sample designs did not allow projection of the test results to the universe from which the samples were selected.

Computer-Processed Data

During our audit, we obtained data from JMD and FBI systems. We did not test the reliability of those systems as a whole, therefore any findings identified involving information from those systems were verified with documentation from other sources.

APPENDIX 2: Notable Federal C-SCRM Guidance

Organization		Criteria (Date)	Synopsis
NIST	National Institute of Standards and Technology (NIST)	NIST 800-161: Supply Chain Risk Management Practices for Federal Information Systems and Organizations (2015) and Revision 1 (2022)	Provides guidance to federal agencies on identifying, assessing, selecting, and implementing risk management processes and mitigating controls throughout their organizations to help manage cyber supply chain risks. Contains foundational C-SCRM practices, such as using a risk management process that includes criticality, threat, and vulnerability analyses. In May 2022, NIST released Revision 1, which contains key practices for organizations to adopt as they develop their capability to manage cybersecurity risks within and across their supply chains.
	Federal Bureau of Investigation (FBI)	Best Practices in C-SCRM for the U.S. Government (2016)	FBI's response to a congressional requirement that it develop best practices for supply chain risk management. States that federal agencies should develop a C-SCRM strategy that accounts for known and emerging threats, vulnerabilities, and organizational impacts. Contains recommendations for developing a supply chain risk assessment and neutralizing risks to an acceptable level.
	Office of Management and Budget (OMB)	Circular A-130 Managing Information as a Strategic Resource (2016)	States that agencies shall consider supply chain security issues for all resource planning and management activities throughout the system development lifecycle; and shall implement C-SCRM principles to protect against counterfeits, unauthorized production, tampering, theft, insertion of malicious software, etc.
	Committee on National Security Systems (CNSS)	Committee on National Security Systems Directive 505 - Supply Chain Risk Management (2021)	Provides guidance for organizations that own, operate, or maintain national security systems (NSS) to address supply chain risk, and implement and sustain C-SCRM capabilities. States that U.S. government departments and agencies will maintain an organizational C-SCRM program to identify, assess, and mitigate supply chain risk to NSS, components, and associated services. This version superseded the previous version from 2017.
	National Counterintelligence and Security Center (NCSC)	Intelligence Community Directive 731 - Supply Chain Risk Management; and Associated Standards (2013-2019)	Intelligence community policy to protect the supply chain for mission-critical products, materials, and services through the identification, assessment, and mitigation of threats. Includes five associated standards on mission-criticality, threat assessments, vulnerability assessments, overall risk assessments, and information-sharing.
	U.S. Congress	The Federal Acquisition Supply Chain Security Act of 2018 (2018)	Established the Federal Acquisition Security Council and contains executive agency C-SCRM requirements including developing an overall C-SCRM strategy and implementation plan and sharing relevant information with other executive agencies.

Source: OIG, based on information from the above resources

APPENDIX 3: Intelligence Community Standard 731 Requirements

Rating	IC Standard 731-02 Threat Levels and Definitions	IC Standard 731-04 Vulnerability Ratings & Definitions	IC Standard 731-05 Impact Levels and Definitions
CRITICAL 	Information indicates a foreign intelligence entity (FIE), or other adversary is engaged in subversion, exploitation, or sabotage of the acquisition item or service's supply chain, including business practices and relationships. Alternatively, information indicates an FIE or other adversary has established an overt or clandestine relationship within the supply chain, and that an FIE or other adversary has the capability and intent to engage in subversion, exploitation, or sabotage of the acquisition item or service's supply chain.	The vulnerability is wholly exposed and is easily exploitable by a threat actor with modest capability and resources.	Exercise or exploitation of the vulnerability would cause total mission failure or other catastrophic effects that are either unrecoverable or could only be recovered from with exceptional time and resources.
HIGH 	Information indicates a FIE or other adversary has the capability and intent to engage in subversion, exploitation or sabotage of the acquisition item or service's supply chain; however, there are no indications of subversion, exploitation, or sabotage.	The vulnerability is highly exposed and is reasonably exploitable by a threat actor with modest capability and resources.	Exercise or exploitation of the vulnerability would cause severe adverse effects on organizations, individuals, or missions resulting in the need for significant time and resources to recover.
MEDIUM 	Information indicates a FIE or other adversary has either the capability or intent to engage in subversion, exploitation or sabotage of the acquisition item or service's supply chain; however, there are no indications of subversion, exploitation, or sabotage.	The vulnerability is moderately exposed and a threat actor with modest with modest capability and resources would face difficulties in trying to exploit it.	Exercise or exploitation of the vulnerability would cause serious adverse effects on organizations, individuals, or missions that can be readily and quickly managed with no long-term consequences.
LOW 	Information indicates FIEs or other adversaries have neither the capability nor the intent to engage in subversion, exploitation, or sabotage of the acquisition item or service's supply chain.	The vulnerability is not exposed and a threat actor with modest capability and resources would unlikely be able to exploit it.	Exercise or exploitation of the vulnerability would have very little adverse effect on organizations, individuals, or missions; and any adverse effects can be readily and quickly managed.
INSUFFICIENT INFO. 	The information available is insufficient to assign a threat level to a FIE' s or other adversary's capability and intent to engage in subversion, exploitation, or sabotage of the acquisition item or service's supply chain.	Not Applicable	Not Applicable

Source: OIG, based on Intelligence Community Standards 731-02, 731-04, & 731-05

APPENDIX 4: Justice Management Division Response to the Draft Report

U.S. Department of Justice

Washington, D.C.

MEMORANDUM FOR JASON R. MALMSTROM
ASSISTANT INSPECTOR GENERAL FOR AUDIT
OFFICE OF THE INSPECTOR GENERAL

FROM: Melinda Rogers
Deputy Assistant Attorney General
Chief Information Officer

MELINDA ROGERS Digitally signed by MELINDA ROGERS Date: 2022.06.15 15:10:01 -04'00'

SUBJECT: JMD Response Letter to Cyber Supply Chain Risk Management Audit

JMD has reviewed the recommendations contained in the Office of the Inspector General draft audit report titled, *Audit of the Department's Cyber Supply Chain Risk Management Efforts.* JMD is pleased to provide its response to the recommendations made in the report. This letter addresses the recommendations that were made to JMD or jointly to JMD and FBI.

Recommendation 1: Coordinate with the BOP and FPI, EOUSA, JMD, NSD, and USMS, and other Department components that are subject to JMD's C-SCRM requirements and whose compliance statuses are unknown, to ensure they maintain or develop the procedures and controls necessary to comply with JMD's C-SCRM requirements; incorporate into its C-SCRM program steps to monitor and verify Department compliance with its guidance through periodic outreach, communication, and the establishment of internal controls; and enhance Department awareness of its C-SCRM program, such as through training.

Response: Concur. JMD will coordinate with other Department components to raise awareness of C-SCRM requirements. C-SCRM topics, including development of the DOJ C-SCRM strategy document, have been briefed regularly at DOJ Cybersecurity Committee and CIO Council meetings. SCRM training has been incorporated into annual awareness training for all DOJ users. Additional training on SCRM requirements has been incorporated into DOJ Information Technology Professional Training, which is required for privileged users and other specialized IT roles.

Recommendation 2: Ensure that its C-SCRM strategy consolidates the existing requirements, including for wireless communications platforms; is refreshed periodically to reflect the latest requirements, standards, and best practices; includes a periodic re-assessment of the Department systems that are most vulnerable or that would cause the greatest organizational impact if compromised; and includes processes that better promote transparency and communication of C-SCRM results to Department components.

Response: Concur. JMD has developed and published a C-SCRM strategy, which will be periodically updated.

Recommendation 3: Update its C-SCRM risk assessment methodology to assess vulnerabilities, likelihood, and impact, in accordance with NIST 800-161, Revision 1 and CNSS Directive 505; and that its risk assessment also be applied to resellers, particularly those handling IT goods.

Response: Concur. JMD is currently analyzing updates to the assessment methodology to enhance the risk assessment approach in alignment with NIST 800-161.

Recommendation 4: Develop policies and procedures that enable it to establish viable mitigation options that are descriptive, actionable, and tailored to the user environment and operational contexts, to be included in risk determination letters as needed; and that it establishes internal controls to monitor Department fulfillment of the mitigating actions.

Response: Concur. JMD will update the risk determination letters to include tailored mitigations.

Recommendation 15: Ensure that ASU updates its vendor threat assessment process to incorporate IC Standard 731-02's required threat level definitions, and that JMD adopts the FBI's revised approach to ensure intra-Department consistency.

Response: Concur. JMD will coordinate with the FBI ASU as the vendor threat assessment methodology is updated.

Recommendation 16: Establish policies, procedures, and internal controls that ensure they follow Congressional requirements to apply C-SCRM procedures to new FISMA reportable IT systems designated high- or moderate-impact and report C-SCRM statistics to the OIG. FBI and JMD should also contact CNSS to determine if submission of an annual report on the progress and effectiveness of their C-SCRM capabilities remains an active requirement, and if so, establish policies and procedures to ensure that they submit—either separately or jointly—these reports to CNSS annually, in accordance with CNSS Directive 505.

Response: Concur. JMD has begun coordination with the Information Technology Acquisition Review process to ensure all applicable procurements, including new FISMA reportable systems that are high- or moderate-impact, follow C-SCRM processes. JMD is also implementing the NIST Special Publication 800-53 Rev 5 controls for supply chain risk management for all applicable DOJ information systems. JMD will contact CNSS to determine annual SCRM reporting requirements.

Recommendation 17: Assess how it can better share C-SCRM information within the Department and identify opportunities to bolster C-SCRM information sharing with other federal agencies.

Response: Concur. JMD has identified several mechanisms to better share C-SCRM information with DOJ components, including DOJ CIO Council, DOJ Cybersecurity Committee,

and the operational sync meetings, which are held with the Justice Security Operations Center and component security representatives. DOJ also participates in the Federal Acquisition Security Council for government-wide C-SCRM information sharing and coordination.

APPENDIX 5: Executive Office for U.S. Attorneys Response to the Draft Report

U.S. Department of Justice

Executive Office for United States Attorneys

Office of the Director

Room 2261, RFK Main Justice Building
950 Pennsylvania Avenue, NW
Washington, DC 20530

(202) 252-1000

MEMORANDUM

DATE: June 27, 2022

FOR: Kimberly L. Rice
Regional Audit Manager
Denver Regional Audit Office
Office of the Inspector General

FROM: Monty Wilkinson
Director

SUBJECT: Amended Response to the Inspector General's Final Draft Report for the *Audit of the Department's Cyber Supply Chain Risk Management Efforts*

CONTACT PERSON: EOUSA Audit Liaison
USAEO.EOUSA.Audit.Liaison@usdoj.gov

The Executive Office for United States Attorneys (EOUSA) appreciates the opportunity to review the Office of the Inspector General's (OIG) final draft report titled, *Audit of the Department's Cyber Supply Chain Risk Management Efforts*, and provides the following response to the recommendation that involves EOUSA. This response is consistent with EOUSA's initial response submitted on June 1. However, after further review of the final draft report and discussion with OIG, EOUSA no longer has sensitivity concerns with the report.

Recommendation No. 1: Coordinate with the BOP and FPI, EOUSA, JMD, NSD, and USMS, and other Department components that are subject to JMD's C-SCRM requirements and whose compliance statuses are unknown, to ensure they maintain or develop the procedures and controls necessary to comply with JMD's C-SCRM requirements; incorporate into its C-SCRM program steps to monitor and verify Department compliance with its guidance through periodic outreach, communication, and the establishment of internal controls; and enhance Department awareness of its C-SCRM program, such as through training.

EOUSA Response: EOUSA concurs with this recommendation. EOUSA will designate a focal point to lead and coordinate EOUSA's SCRM program compliance with JMD's SCRM requirements. EOUSA will implement a SCRM program and work to provide the required governance, processes, and tools to effectively assess supply chain risk for United States Attorneys' IT acquisitions by the end of fiscal year 2023. EOUSA will continue providing guidance and support regarding SCRM requirements through training and awareness campaigns while simultaneously working towards its program implementation.

If you have further questions or requests, please contact EOUSA's Audit Liaison at the contact information provided above.

APPENDIX 6: Drug Enforcement Administration Response to the Draft Report

U. S. Department of Justice
Drug Enforcement Administration

www.dea.gov

MEMORANDUM

TO: Kimberly L. Rice
Regional Audit Manager
Denver Regional Audit Office

FROM: Mary B. Schaefer
Chief Compliance Officer
Office of Compliance

MARY SCHAEFER Digitally signed by MARY SCHAEFER Date: 2022.06.03 17:42:53 -04'00'

SUBJECT: Drug Enforcement Administration (DEA) Response Memorandum re: "Audit of the Department's Cyber Supply Chain Risk Management Efforts (Draft Report and Recommendation #5)"

On May 20, 2022, the Department of Justice (DOJ), Office of the Inspector General (OIG) issued the "Audit of the Department's Cyber Supply Risk Management Efforts (C-SCRM)" draft report. In the draft report, OIG made one recommendation (Recommendation #5) to improve the Drug Enforcement Administration's (DEA) oversight of the C-SCRM process within the DEA's Office of National Security Information (ONSI), the only Intelligence Community (IC) element within the agency. This memorandum describes DEA's plans to address the recommendation.

Recommendation 5: We recommend that the DEA establish policies and procedures to ensure ONSI compliance with Intelligence Community Directive 731 and its associated standards.

DEA Response:

The DEA concurs with the recommendation. ONSI will address this recommendation as follows:

1) To ensure compliance with IC Directive (ICD) 731 and its associated standards, ONSI will continue participating in the DOJ, Justice Management Division (JMD) C-SCRM program. On an annual basis, ONSI makes one, or a maximum of two, purchases that are required to go through the C-SCRM process. DEA considered establishing its own C-SCRM program, but determined that doing so was not feasible because of limited resources (personnel and funding). DEA understands that JMD will implement OIG's recommendations and is confident in continuing with JMD's C-SCRM program.

2) ONSI is developing a new standalone policy in which it will detail the requirements that all ONSI personnel must follow to comply with the ICD 731 and ONSI's established C-SCRM process. This effort is on-going and, once completed, DEA will provide OIG with a copy of its new policy and request that it close this recommendation once DEA has approved and published its new policy.

If you have any questions or concerns regarding DEA's response, please contact Section Chief Don R. Berthiaume at (202) 316-2174.

Cc: Louise Duhamel
Assistant Director
Audit Liaison Group
Internal Review and Evaluation Office

APPENDIX 7: Federal Bureau of Investigation Response to the Draft Report

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

June 10, 2022

The Honorable Michael E. Horowitz
Inspector General
Office of the Inspector General
U.S. Department of Justice
950 Pennsylvania Avenue, N.W.
Washington, DC 20530

Dear Mr. Horowitz:

The Federal Bureau of Investigation (FBI) appreciates the opportunity to review and respond to your office's report entitled, *Audit of the Department's Cyber Supply Chain Risk Management Efforts.*

We are glad you found that the FBI has made significant progress towards modernizing and operating its cyber supply chain risk management (C-SCRM) program. We also understand you found several areas in which the management of the FBI's C-SCRM program can be improved. In that regard, we concur with your twelve recommendations for the FBI.

Should you have any questions, feel free to contact me. We greatly appreciate the professionalism of your audit staff throughout this matter.

Sincerely,

Suzanne Turner
Assistant Director
Inspection Division

Enclosure

The Federal Bureau of Investigation's (FBI) Response to the Office of the Inspector General's Audit of the Department's Cyber Supply Chain Risk Management Efforts

OIG Final Draft Recommendation 6: Enhance its policies, procedures, training and communication, and/or internal controls for the requisition and government purchase card systems to better ensure that purchasing officials understand the C-SCRM requirements and so that applicable requisitions and purchase requests undergo C-SCRM procedures, as required; and develop policies, procedures, and/or internal controls to periodically monitor FBI compliance by identifying and remedying purchases that improperly bypassed the process.

FBI Response: The FBI concurs with the recommendation. The FBI self-recognized the importance of C-SCRM and assessed the FBI's current procurement application, Automated Requisition Tool's (ART) limitations in the C-SCRM area. As a result, the FBI developed the Standard Hub for Ordering and Purchasing (SHOP) and has begun the early stages of transition from ART, providing SHOP demos, trainings and pilot transactions. The FBI continues to develop and enhance SHOP capabilities and is working to include controls that will require applicable requisitions to go through the SCRM process before moving to the next phase of the requisition process.

OIG Final Draft Recommendation 7: Ensure that Acquisition Security Unit analysts receive the training and resources necessary to fulfill IC Standard 731-02's sourcing requirements and that ASU then incorporates the IC Directive 206 sourcing procedures into its vendor threat assessment process; that ASU and the SCRM Unit modify the existing vendor threat assessment process to better align its information collection methodology, risk tolerance levels, and other attributes with the enterprise needs; and that ASU develops policies or procedures to ensure that ASU vendor threat assessments, especially those for high or critical risk vendors, are updated every 2 years, as required by IC Directive 731.

FBI Response: The FBI concurs with the recommendation. The FBI plans to work with the Directorate of Intelligence and Training Division coordinators to identify applicable standard courses that are available to Acquisition Security Unit (ASU) employees specific to IC Directive 206 sourcing procedures. Once courses are identified, ASU employees will be required to complete them within 90 days.

ASU and Supply Chain Risk Management Unit (SCRMU) will continue to work together to identify a method in which requisitions can be reviewed in advance to determine if the IT product requires a Company Threat Assessment (CTA). Additionally, with the implementation of the Standard Hub for Ordering and Procuring (SHOP) platform, each Unit will be able to work congruently to complete required actions.

ASU plans to work with Resource Planning Office (RPO) to build a mechanism within SHOP that will identify all CTAs that are within 3 months of the expiration date. Once the CTAs are identified, they will be assigned to an ASU analyst to update within the standard 2 year requirement.

OIG Final Draft Recommendation 8: Improve the product vulnerability assessments for mission-critical ICT products by incorporating necessary information from the vendor threat assessments, evaluating vulnerabilities and the ease of exploitability by a threat actor, identifying whether specific mitigations exist to address product vulnerabilities, and assigning a vulnerability rating to each vulnerability identified, to better align the product vulnerability assessment with IC Standard 731-04.

FBI Response: The FBI concurs with the recommendation. SCRMU and ASU leadership will provide training on IC Directive 206 and IC Standard 731-04 to SCRMU and ASU employees. SCRMU has developed and is utilizing a criticality process flow that aligns with ICD 731-04. SCRMU is also establishing a standing C-SCRM Working Group made up of units from multiple FBI divisions (including OCIO, SecD, FFD, CD, CyD, and others as necessary) to work through current and ongoing C-SCRM challenges. The working group will work together to ensure CTAs and other C-SCRM documentation meets ICD/NIST standards. ASU is working to establish a proactive update for commonly requested critical vendor threat assessments.

OIG Final Draft Recommendation 9: Improve the procurement risk assessment for mission-critical ICT products by incorporating necessary information from the vendor threat and product vulnerability assessments; complete likelihood and impact analyses for identified vulnerabilities, including assigning likelihood and impact ratings; and document an overall risk score for the procurement, to better align the procurement risk assessment with IC Standard 731-05.

FBI Response: The FBI concurs with the recommendation. SCRMU is establishing capabilities and procedures to secure appropriate intelligence from the FBI Intelligence Branch to support likelihood/impact assessments and to help bolster/validate threat assessments. The FBI Intelligence Branch is also working on the creation of country-based capabilities products to be used in the development of likelihood ratings. The C-SCRM Working Group will also focus efforts to ensure FBI vulnerability assessments align more with ICD 731-05.

OIG Final Draft Recommendation 10: Work with OCIO and the SCRM Unit to track and document ICT product procurement re-direct decisions in order to properly report these procurements to Congress, better improve compliance with IC Standard 731-04, and enhance the FBI's capability to ensure that high-risk products do not bypass C-SCRM processes.

FBI Response: The FBI concurs with the recommendation. SCRMU is currently tracking monthly reports of redirects on critical companies and documenting them. SCRMU is also providing these reports to Security Division (SECD) for their information and understanding. SCRMU will work with ASU to ensure all necessary reporting to Congress and other appropriate authorities is completed.

OIG Final Draft Recommendation 11: Ensure mitigation actions for ICT products, especially mission-critical ICT products or services, are descriptive, actionable, and tailored to the user environment and operational contexts (including its anonymity of procurement statement); and work with OCIO and the SCRM Unit to create and resource a continuous monitoring program that monitors C-SCRM risks across the FBI, ensures that users understand and follow C-SCRM mitigations identified in the product vulnerability and procurement risk assessments, and

develops procedures to periodically monitor and assess user compliance with its C-SCRM mitigation actions.

FBI Response: The FBI concurs with the recommendation. SCRMU has created custom risk assessment documentation for critical items that allows for a more transparent and repeatable process, tracking of redirects and rejections, and notifications of approvals. It has also developed an FBI risk assessment process that aligns with ICD 731-04. SCRMU is working with FFD to secure a continuous monitoring tool to proactively notify the team of business intelligence and risk. SCRMU expects this tool to be implemented by the end of FY22. SCRMU is working with the Audit Unit to establish a SCRM Audit Program that can effectively evaluate the completion of critical mitigation plans. SCRMU has also established relationships with affected system ISSOs and ISSMs to establish measurable and actionable mitigation plans for procurements when necessary.

OIG Final Draft Recommendation 12: Better integrate its C-SCRM program across the enterprise and leverage other FBI units that help inform and apply the required processes and risk decisions, such as through the use of a
Program Management Office or similar operating model that is led by an accountable FBI executive level official.

FBI Response: The FBI concurs with the recommendation. SCRMU is establishing a standing C-SCRM Working Group made up of units from multiple FBI divisions (including OCIO, SecD, FFD, CD, CyD, and others as necessary) to work through current and ongoing C-SCRM challenges.

OIG Final Draft Recommendation 13: Establish policies and procedures to evaluate, certify, and submit reports to the Assistant Director of National Intelligence for Acquisition, Technology, and Facilities on the integrity of its organizational supply chain processes every 2 years, in accordance with IC Directive 731.

FBI Response: The FBI concurs with the recommendation. SCRMU has developed the FBI SCRM Transition Plan Outline. This plan will help to mature the current CSCRM process, ensure greater participation in "whole of government" C-SCRM information sharing, ensure compliance with NIST and ICD policy and directive where required, apply internal knowledge bases more effectively, and audit FBI customer compliance to provided mitigation plans. SCRMU is working with other FBI divisions to establish a standing C-SCRM Working Group made up of units from multiple FBI divisions to work through current and ongoing C-SCRM challenges. The C-SCRM Working Group members will verify C-SCRM reporting from the appropriate FBI divisions is completed.

OIG Final Draft Recommendation 14: Designate a senior official from the OCIO as its representative for, and who actively participates on, the Supply Chain and Counterintelligence Risk Management Task Force.

FBI Response: The FBI concurs with the recommendation. The Section Chief for the OCIO Enterprise Technology Services Section (ETSS) will be the accountable executive for the SCCRMTF.

OIG Final Draft Recommendation 15: Ensure that ASU updates its vendor threat assessment process to incorporate IC Standard 731-02's required threat level definitions, and that JMD adopts the FBI's revised approach to ensure intra-Department consistency.

FBI Response: The FBI concurs with the recommendation. The FBI has identified the following threat level definitions located in IC Standard 731-02 and will integrate them into the threat assessment process:

Critical- Information indicated Foreign Intelligence Entities (FIE) or other adversary is engaged in subversion, exploitation or sabotage of the acquisition item or service's supply chain, including business practices and relationships. Alternatively, information indicates a FIE or other adversary has established an overt or clandestine relationship within the supply chain, and that a FIE or other adversary has the capability and intent to engage in subversion, exploitation, or sabotage of the acquisition item or service's supply chain.

High- Information indicates a FIE or other adversary has the capability and intent to engage in subversion, exploitation or sabotage of the acquisition item or service's supply chain, however, there are no indication of subversion, exploitation or sabotage.

Medium- Information indicates a FIE or other adversary has either the capability or intent to engage in subversion, exploitation or sabotage of the acquisition items or service's supply chain, however, there are no indications of subversion, exploitation or sabotage.

Low-Information indicates FIE's or other adversaries have neither the capability nor the intent to engage in subversion, exploitation or sabotage of the acquisition item or service's supply chain.

Insufficient information- The information available is insufficient to assign a threat level to a FIE or other adversary's capability and intent to engage in subversion, exploitation, or sabotage of the acquisition item or service's supply chain.

FBI will coordinate with JMD to ensure JMD adopts the FBI's revised approach in usage of the IC Standard 731-02's required threat level definitions.

OIG Final Draft Recommendation 16: Establish policies, procedures, and internal controls that ensure they follow Congressional requirements to apply C-SCRM procedures to new FISMA reportable IT systems designated high- or moderate-impact and report C-SCRM statistics to the OIG. FBI and JMD should also contact CNSS to determine if submission of an annual report on the progress and effectiveness of their C-SCRM capabilities remains an active requirement, and if so, establish policies and procedures to ensure that they submit—either separately or jointly—these reports to CNSS annually, in accordance with CNSS Directive 505.

FBI Response: The FBI concurs with the recommendation. The C-SCRM Working Group members will verify that appropriate FBI divisions complete any current or additional reporting requirements, while also sharing findings with JMD.

OIG Final Draft Recommendation 17: Assess how it can better share C-SCRM information within the Department and identify opportunities to bolster C-SCRM information sharing with other federal agencies.

FBI Response: The FBI concurs with the recommendation. The C-SCRM Working Group members will develop and implement a process to ensure appropriate information sharing for C-SCRM information when legal and appropriate.

APPENDIX 8: Office of the Inspector General Analysis and Summary of Actions Necessary to Close the Report

The OIG provided a draft of this audit report to the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF); Drug Enforcement Administration (DEA); Executive Office for U.S. Attorneys (EOUSA); Federal Bureau of Investigation (FBI); Federal Bureau of Prisons (BOP) and Federal Prison Industries, Inc. (FPI); Justice Management Division (JMD); National Security Division (NSD); and U.S. Marshals Service (USMS). Component responses are incorporated into Appendices 4 through 7 of this final report.[67] The respondents concurred with our recommendations and discussed the actions they will implement in response to our findings. As a result, the status of this audit report is resolved. The following provides the OIG analysis of the responses and summary of actions necessary to close the report.

Recommendations for JMD:

1. **Coordinate with the BOP and FPI, EOUSA, JMD, NSD, and USMS, and other Department components that are subject to JMD's C-SCRM requirements and whose compliance statuses are unknown, to ensure they maintain or develop the procedures and controls necessary to comply with JMD's C-SCRM requirements; incorporate into its C-SCRM program steps to monitor and verify Department compliance with its guidance through periodic outreach, communication, and the establishment of internal controls; and enhance Department awareness of its C-SCRM program, such as through training.**

   Resolved. JMD concurred with our recommendation. JMD stated that it would coordinate with other Department components to raise awareness of the C-SCRM requirements; and that C-SCRM topics, including the development of the Department C-SCRM strategy document, have been discussed at the DOJ Cybersecurity Committee and CIO Council meetings. JMD also noted that C-SCRM has been incorporated into both its annual awareness training for all users, and its IT Professional training for privileged users and personnel with specialized IT roles.

   Additionally, EOUSA provided a written response, stating that it will designate a focal point to lead and coordinate its compliance with JMD's C-SCRM requirements. EOUSA added that it will implement a C-SCRM program and work to provide the required governance, processes, and tools to effectively assess supply chain risk for U.S. Attorneys' IT acquisitions by the end of FY 2023. Lastly, EOUSA noted that while implementing its C-SCRM program, it would also provide guidance and support through training and awareness campaigns.

   This recommendation can be closed when we receive evidence that JMD coordinated with the BOP and FPI, EOUSA, JMD, NSD, and USMS, and other Department components that are subject to JMD's C-SCRM requirements and whose compliance statuses are unknown, to ensure they maintain or develop the procedures and controls necessary to comply with JMD's C SCRM requirements; incorporated into its C-SCRM program steps to monitor and verify Department compliance with its guidance through periodic outreach, communication, and the establishment of internal controls;

[67] FBI, DEA, JMD, and EOUSA provided written responses to this report, which are contained in the prior Appendices.

and enhanced Department awareness of its C-SCRM program, such as through training. For the training aspect of this recommendation, we request JMD provide evidence that the IT Professional training has been provided to privileged and specialized IT users.

2. **Ensure that its C-SCRM strategy consolidates the existing requirements, including for wireless communications platforms; is refreshed periodically to reflect the latest requirements, standards, and best practices; includes a periodic re-assessment of the Department systems that are most vulnerable or that would cause the greatest organizational impact if compromised; and includes processes that better promote transparency and communication of C-SCRM results to Department components.**

   Resolved. JMD concurred with our recommendation. JMD stated that it has developed and published a C-SCRM strategy, which will be periodically updated.

   This recommendation can be closed when JMD provides evidence that its C-SCRM strategy consolidates the existing requirements, including for wireless communications platforms; will be refreshed periodically to reflect the latest requirements, standards, and best practices; includes a periodic re-assessment of the Department systems that are most vulnerable or that would cause the greatest organizational impact if compromised; and includes processes that better promote transparency and communication of C-SCRM results to Department components.

3. **Update its C-SCRM risk assessment methodology to assess vulnerabilities, likelihood, and impact, in accordance with NIST 800-161, Revision 1 and CNSS Directive 505; and that its risk assessment also be applied to resellers, particularly those handling IT goods.**

   Resolved. JMD concurred with our recommendation. JMD stated that it is currently analyzing updates to the assessment methodology to enhance the risk assessment approach in alignment with NIST 800-161.

   This recommendation can be closed when JMD provides evidence that it updated its C-SCRM risk assessment methodology to assess vulnerabilities, likelihood, and impact, in accordance with NIST 800-161, Revision 1 and CNSS Directive 505; and that its risk assessment also be applied to resellers, particularly those handling IT goods.

4. **Develop policies and procedures that enable it to establish viable mitigation options that are descriptive, actionable, and tailored to the user environment and operational contexts, to be included in risk determination letters as needed; and that it establishes internal controls to monitor Department fulfillment of the mitigating actions.**

   Resolved. JMD concurred with our recommendation. JMD stated that it will update the risk determination letters to include tailored mitigations.

   This recommendation can be closed when JMD provides evidence that it developed policies and procedures that enable it to establish viable mitigation options that are descriptive, actionable, and

tailored to the user environment and operational contexts, to be included in risk determination letters as needed; and that it established internal controls to monitor Department fulfillment of the mitigating actions.

Recommendation for the DEA:

5. Establish policies and procedures to ensure ONSI compliance with Intelligence Community Directive 731 and its associated standards.

Resolved. The DEA concurred with our recommendation. The DEA stated that ONSI initially considered establishing its own C-SCRM program, but concluded that doing so was infeasible due to its limited resources (personnel and funding). Instead, ONSI intends to continue its participation in JMD's C-SCRM program and is developing a new standalone policy with requirements that all ONSI personnel must follow to comply with Intelligence Community Directive 731 and ONSI's established C-SCRM process.

This recommendation can be closed when we receive a copy of ONSI's new standalone C-SCRM policy and any other applicable evidence demonstrating that ONSI is ensuring compliance with Intelligence Community Directive 731 and its associated standards.

Recommendations for the FBI:

6. Enhance its policies, procedures, training and communication, and/or internal controls for the requisition and government purchase card systems to better ensure that purchasing officials understand the C-SCRM requirements and so that applicable requisitions and purchase requests undergo C-SCRM procedures, as required; and develop policies, procedures, and/or internal controls to periodically monitor FBI compliance by identifying and remedying purchases that improperly bypassed the process.

Resolved. The FBI concurred with our recommendation. The FBI acknowledged that its former requisition system contained C-SCRM limitations, but that it was transitioning to a newly developed replacement called the Standard Hub for Ordering and Purchasing (SHOP) and has begun the early stages of transition, providing SHOP demonstrations, trainings and pilot transactions. The FBI stated that SHOP will include controls requiring applicable requisitions undergo the C-SCRM process before moving to the next phase of the requisition process.

This recommendation can be closed when we receive evidence that the FBI has enhanced its policies, procedures, training and communication, and/or internal controls for the requisition and government purchase card systems to better ensure that purchasing officials understand the C-SCRM requirements and so that applicable requisitions and purchase requests undergo C-SCRM procedures, as required; and develop policies, procedures, and/or internal controls to periodically monitor FBI compliance by identifying and remedying purchases that improperly bypassed the process.

7. **Ensure that Acquisition Security Unit analysts receive the training and resources necessary to fulfill IC Standard 731-02's sourcing requirements and that ASU then incorporates the IC Directive 206 sourcing procedures into its vendor threat assessment process; that ASU and the SCRM Unit modify the existing vendor threat assessment process to better align its information collection methodology, risk tolerance levels, and other attributes with the enterprise needs; and that ASU develops policies or procedures to ensure that ASU vendor threat assessments, especially those for high or critical risk vendors, are updated every 2 years, as required by IC Directive 731.**

   Resolved. The FBI concurred with our recommendation. The FBI stated that the Directorate of Intelligence and Training Division will help identify courses on IC Directive 206 sourcing procedures for ASU employees. ASU employees will then be required to complete the identified courses within 90 days. The FBI also stated that ASU and the SCRM Unit will collaborate to determine if the IT product requires a vendor threat assessment, and that the newly developed SHOP platform will enable ASU and the SCRM Unit to work congruently to complete required actions. Lastly, the FBI stated that ASU and the Resource Planning Office plan to build a mechanism within SHOP that will identify vendor threat assessments that are within 3 months of expiration.

   This recommendation can be closed when we receive evidence that ASU analysts receive the training and resources necessary to fulfill IC Standard 731-02's sourcing requirements and that ASU then incorporates the IC Directive 206 sourcing procedures into its vendor threat assessment process; that ASU and the SCRM Unit modify the existing vendor threat assessment process to better align its information collection methodology, risk tolerance levels, and other attributes with the enterprise needs; and that ASU develops policies or procedures to ensure that ASU vendor threat assessments, especially those for high or critical risk vendors, are updated every 2 years, as required by IC Directive 731.

8. **Improve the product vulnerability assessments for mission-critical ICT products by incorporating necessary information from the vendor threat assessments, evaluating vulnerabilities and the ease of exploitability by a threat actor, identifying whether specific mitigations exist to address product vulnerabilities, and assigning a vulnerability rating to each vulnerability identified, to better align the product vulnerability assessment with IC Standard 731-04.**

   Resolved. The FBI concurred with our recommendation. The FBI stated in its response that ASU and the SCRM Unit will provide training on IC Directive 206 and IC Standard 731-04 to their employees and that the SCRM Unit's newly developed criticality workflow aligns with IC Directive 731-04. The FBI also said it is establishing a standing C-SCRM Working Group comprised of units from multiple FBI divisions to work through C-SCRM challenges. This Working Group will ensure that vendor threat assessments and other C-SCRM documentation meet the intelligence community and NIST standards. Lastly, the FBI said that ASU is working to "establish a proactive update for commonly requested critical vendor threat assessments."

   This recommendation can be closed when we receive evidence that the FBI improved the product vulnerability assessments for mission-critical ICT products by incorporating necessary information from the vendor threat assessments, evaluating vulnerabilities and the ease of exploitability by a threat actor, identifying whether specific mitigations exist to address product vulnerabilities, and

assigning a vulnerability rating to each vulnerability identified, to better align the product vulnerability assessment with IC Standard 731-04.

9. **Improve the procurement risk assessment for mission-critical ICT products by incorporating necessary information from the vendor threat and product vulnerability assessments; complete likelihood and impact analyses for identified vulnerabilities, including assigning likelihood and impact ratings; and document an overall risk score for the procurement, to better align the procurement risk assessment with IC Standard 731-05.**

   Resolved. The FBI concurred with our recommendation. The FBI stated that the SCRM Unit seeks to secure intelligence from the Intelligence Branch to support likelihood and impact assessments and to help validate vendor threat assessments. FBI's Intelligence Branch is also creating country-based capabilities products for use in the likelihood ratings. Lastly, the FBI said the C-SCRM Working Group will ensure that FBI vulnerability assessments better align with IC Standard 731-05.

   This recommendation can be closed when we receive evidence that the FBI improved the procurement risk assessment for mission-critical ICT products by incorporating necessary information from the vendor threat and product vulnerability assessments; completed likelihood and impact analyses for identified vulnerabilities, including assigning likelihood and impact ratings; and documented an overall risk score for the procurement, to better align the procurement risk assessment with IC Standard 731-05.

10. **Work with OCIO and the SCRM Unit to track and document ICT product procurement re-direct decisions in order to properly report these procurements to Congress, better improve compliance with IC Standard 731-04, and enhance the FBI's capability to ensure that high-risk products do not bypass C-SCRM processes.**

    Resolved. The FBI concurred with our recommendation. The FBI stated that the SCRM Unit is currently tracking monthly reports of re-directs on critical companies and sharing these reports with the Security Division for their information and understanding. The FBI noted that the SCRM Unit will work with ASU to ensure all necessary reporting to Congress and other appropriate authorities is completed.

    This recommendation can be closed when we receive evidence that the FBI tracks and documents ICT product procurement re-direct decisions in order to properly report these procurements to Congress, better improve compliance with IC Standard 731-04, and enhance the FBI's capability to ensure that high-risk products do not bypass C-SCRM processes.

11. **Ensure mitigation actions for ICT products, especially mission-critical ICT products or services, are descriptive, actionable, and tailored to the user environment and operational contexts (including its anonymity of procurement statement); and work with OCIO and the SCRM Unit to create and resource a continuous monitoring program that monitors C-SCRM risks across the FBI, ensures that users understand and follow C-SCRM mitigations identified in the product vulnerability and procurement risk assessments, and develops procedures to periodically monitor and assess user compliance with its C-SCRM mitigation actions.**

Resolved. The FBI concurred with our recommendation. The FBI stated that the SCRM Unit has created custom risk assessment documentation for critical items that allows for a more transparent and repeatable process, and the tracking of redirects, rejections, and approvals. SCRM Unit is working with FBI's Finance and Facilities Division to secure a continuous monitoring tool, to be implemented by the end of FY 2022 to proactively notify the team of business intelligence and risk. SCRM Unit is also working with the FBI's Audit Unit to establish a C-SCRM Audit Program that can effectively evaluate the completion of critical mitigation plans. Lastly, the SCRM Unit has established relationships with affected Information System Security Officers and Information System Security Managers to establish measurable and actionable mitigation plans for procurements, when necessary.

This recommendation can be closed when we receive evidence that the FBI ensures that mitigation actions for ICT products, especially mission-critical ICT products or services, are descriptive, actionable, and tailored to the user environment and operational contexts (including its anonymity of procurement statement); and works with OCIO and the SCRM Unit to create and resource a continuous monitoring program that monitors C-SCRM risks across the FBI, ensures that users understand and follow C-SCRM mitigations identified in the product vulnerability and procurement risk assessments, and develops procedures to periodically monitor and assess user compliance with its C-SCRM mitigation actions.

12. **Better integrate its C-SCRM program across the enterprise and leverage other FBI units that help inform and apply the required processes and risk decisions, such as through the use of a Program Management Office or similar operating model that is led by an accountable FBI executive-level official.**

Resolved. The FBI concurred with our recommendation. The FBI stated that the SCRM Unit is establishing a standing C-SCRM Working Group comprised of units from multiple FBI divisions to work through C-SCRM challenges.

This recommendation can be closed when we receive evidence that the FBI's C-SCRM Working Group better integrates the FBI's C-SCRM program across the enterprise, leverages other FBI units that help inform and apply the required processes and risk decisions, and is led by an accountable FBI executive-level official.

13. **Establish policies and procedures to evaluate, certify, and submit reports to the Assistant Director of National Intelligence for Acquisition, Technology, and Facilities on the integrity of its organizational supply chain processes every 2 years, in accordance with IC Directive 731.**

Resolved. The FBI concurred with our recommendation. The FBI stated that the SCRM Unit has developed the "FBI SCRM Transition Plan Outline," which will help mature the current C-SCRM process, ensure greater participation in "whole of government" C-SCRM information sharing; certify compliance with NIST and intelligence community policy and directives, when required; apply internal knowledge bases more effectively; and audit FBI customer compliance with mitigation plans. The FBI stated that it will establish a standing C-SCRM Working Group that will verify that C-SCRM reporting from the appropriate FBI divisions is completed.

This recommendation can be closed when we receive evidence that the FBI established policies and procedures to evaluate, certify, and submit reports to the Assistant Director of National Intelligence for Acquisition, Technology, and Facilities on the integrity of its organizational supply chain processes every 2 years, in accordance with IC Directive 731.

14. **Designate a senior official from the OCIO as its representative for, and who actively participates on, the Supply Chain and Counterintelligence Risk Management Task Force.**

    Resolved. The FBI concurred with our recommendation. The FBI stated that the Section Chief for the OCIO Enterprise Technology Services Section will be the accountable executive for the Supply Chain and Counterintelligence Risk Management Task Force.

    This recommendation can be closed when we receive evidence that the FBI designated the abovementioned OCIO official as its representative for the Supply Chain and Counterintelligence Risk Management Task Force, and evidence that this official actively participates on the task force.

Recommendations for JMD and the FBI:

15. **Ensure that ASU updates its vendor threat assessment process to incorporate IC Standard 731-02's required threat level definitions, and that JMD adopts the FBI's revised approach to ensure intra-Department consistency.**

    Resolved. The FBI and JMD concurred with our recommendation. The FBI stated that it would integrate the IC Standard 731-02 threat level definitions (see Appendix 3 for these definitions) into its vendor threat assessment process, and that it will coordinate with JMD to ensure it adopts the FBI's revised approach. JMD stated that it will coordinate with ASU as the vendor threat assessment methodology is updated.

    This recommendation can be closed when we receive evidence that the FBI updated its vendor threat assessment process to incorporate IC Standard 731-02's required threat level definitions, and that JMD adopted the FBI's revised approach.

16. **Establish policies, procedures, and internal controls that ensure they follow Congressional requirements to apply C-SCRM procedures to new FISMA reportable IT systems designated high- or moderate-impact and report C-SCRM statistics to the OIG. FBI and JMD should also contact CNSS to determine if submission of an annual report on the progress and effectiveness of their C-SCRM capabilities remains an active requirement, and if so, establish policies and procedures to ensure that they submit—either separately or jointly—these reports to CNSS annually, in accordance with CNSS Directive 505.**

    Resolved. The FBI and JMD concurred with our recommendation. The FBI stated that C-SCRM Working Group members will verify that appropriate FBI divisions complete any current or additional reporting requirements, while also sharing findings with JMD. JMD stated that it has begun coordination with the IT Acquisition Review process to ensure all applicable procurements

(including new FISMA reportable systems that are high- or moderate-impact) follow C-SCRM processes. JMD also noted that it is implementing NIST Special Publication 800-53, Revision 5's controls for supply chain risk management for all applicable DOJ information systems; and that it will contact the Committee on National Security Systems to determine annual C-SCRM reporting requirements.

This recommendation can be closed when the FBI and JMD provide evidence that they established policies, procedures, and internal controls that ensure they follow Congressional requirements to apply C SCRM procedures to new FISMA reportable IT systems designated high- or moderate-impact and report C SCRM statistics to the OIG. The FBI and JMD should also provide evidence that they contacted CNSS to determine if submission of an annual report on the progress and effectiveness of their C-SCRM capabilities remains an active requirement, and if so, establish policies and procedures to ensure that they submit—either separately or jointly—these reports to CNSS annually, in accordance with CNSS Directive 505.

17. Assess how it can better share C-SCRM information within the Department and identify opportunities to bolster C-SCRM information sharing with other federal agencies.

Resolved. The FBI and JMD concurred with our recommendation. The FBI stated that the C-SCRM Working Group members will develop and implement a process to ensure appropriate C-SCRM information sharing, when legal and appropriate. JMD stated that it had identified several mechanisms to better share C-SCRM information with Department components, including the Department's CIO Council, Cybersecurity Committee, and the operational sync meetings which are held with the Justice Security Operations Center and component security representatives. JMD also noted that the Department participates in the Federal Acquisition Security Council for government-wide C-SCRM information sharing and coordination.

This recommendation can be closed when the FBI and JMD provide evidence that they assessed how to better share C-SCRM information within the Department and identified opportunities to bolster C-SCRM information sharing with other federal agencies.