TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

More Interim Steps Could Be Taken to Mitigate Information Technology Supply Chain Risks

February 2, 2022

Report Number: 2022-20-009

TIGTACommunications@tigta.treas.gov | www.treasury.gov/tigta

HIGHLIGHTS: More Interim Steps Could Be Taken to Mitigate Information Technology Supply Chain Risks

Final Audit Report issued on February 2, 2022

Report Number 2022-20-009

Why TIGTA Did This Audit

The President and Congress have expressed significant interest in and have taken steps to limit the Government's exposure to supply chain risks. In 2020, there was a significant supply chain incident in which software from the SolarWinds Corporation was breached giving hackers access to thousands of Government agency and private company systems using this software.

This audit was initiated to evaluate the IRS's efforts to identify, assess, and mitigate information technology supply chain risks.

Impact on Taxpayers

Information technology relies on a complex, globally distributed, and interconnected supply chain ecosystem. Commercially available information technology solutions present significant benefits, including low cost, rapid innovation, and a variety of product features and choices. As a result, the Federal Government has rapidly adopted these solutions for its information technology systems and increased its reliance on commercially available products and services. However, the same globalization and other factors that allow for such benefits also increase the risk of a threat event, which can directly or indirectly affect the Government's information technology supply chain.

Weak supply chain risk management (SCRM) controls could potentially compromise the confidentiality, integrity, and availability of the IRS's information systems as well as increase the risk of disruptions to its mission-critical functions.

What TIGTA Found

The Department of the Treasury has overall responsibility for developing the strategy and guidance policies to manage information technology SCRM for the department and its bureaus. It is in the process of finalizing the guidance policies as well as completing internal reviews. The IRS plans to leverage the Department of the Treasury's guidance policies to create its own once they are approved. As a result, the IRS is only in the beginning stages of information technology SCRM planning. The IRS has conducted some initial research on the Internet to understand what other Federal agencies are undertaking and has taken some preliminary steps, such as drafting a strategy and updating policy and guidance, to address information technology supply chain risk.

However, while waiting for the Department of the Treasury, the IRS could take additional steps to better manage and mitigate some information technology supply chain risks in the short term. For example, as part of its information security program planning, the IRS could begin documenting relevant SCRM controls and integrating them into ongoing security assessment and authorization activities.

A review of a judgmental sample of 15 contracts procuring information technology products and services found that contract clauses are not consistently applied to protect the IRS from supply chain risks. For example, 12 of the 14 potential contract clauses addressing supply chain risks were included in some, but not all six, of the contracts procuring software support and maintenance. Similarly, seven of the 14 potential contract clauses addressing supply chain risks were included in some, but not all four, of the contracts procuring comparable services to support application development activities.

What TIGTA Recommended

TIGTA recommended that the Chief Information Officer implement controls to manage information technology supply chain risks based on the revised Internal Revenue Manual guidance as well as do more to identify and incorporate best practices of other Federal agencies that would be applicable to the IRS. The Chief Procurement Officer should ensure that contracting officers are provided further instructions on, and the quality assurance process includes a review for, the proper and consistent application of contract clauses addressing supply chain risks.

The IRS agreed with the recommendations. The Information Technology organization will implement controls to manage information technology supply chain risks based on the revised guidance as well as do more to identify and incorporate applicable SCRM best practices of other Federal agencies. The Office of the Chief Procurement Officer will remind staff and managers on the proper and consistent application of contract clauses addressing supply chain risks and add the identified supply chain risk clauses to its quality assurance review process.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

February 2, 2022

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – More Interim Steps Could Be Taken to Mitigate Information Technology Supply Chain Risks (Audit # 202120021)

This report presents the results of our review to evaluate the Internal Revenue Service's (IRS) efforts to identify, assess, and mitigate information technology supply chain risks. This review is part of our Fiscal Year 2022 Annual Audit Plan and addresses the major management and performance challenge of *Enhancing Security of Taxpayer Data and Protection of IRS Resources*.

Management's complete response to the draft report is included as Appendix II.

Copies of this report are also being sent to the IRS managers affected by the report recommendations. If you have any questions, please contact me or Danny R. Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services).

Table of Contents

Appendices

Background

Information technology relies on a complex, globally distributed, and interconnected supply chain ecosystem that is long, has geographically diverse routes, and consists of multiple tiers of outsourcing.[1] According to National Institute of Standards and Technology (NIST) Special Publication 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*,[2] the supply chain ecosystem "is comprised of entities (*e.g.*, acquirers, system integrators, suppliers, and external service providers) and technology, law, policy, procedures, and practices that interact to design, manufacture, distribute, deploy, and use" information technology products and services. While the ecosystem has evolved to provide a set of highly refined, cost-effective, reusable information technology solutions, it has also increased the complexity, diversity, and scale of information technology supply chains.

Commercially available information technology solutions present significant benefits, including low cost, rapid innovation, a variety of product features, and choices among competing vendors. As a result, the Federal Government has rapidly adopted these solutions for its information technology systems as well as increased its reliance on commercially available products and services. However, the same globalization and other factors that allow for such benefits also increase the risk of a threat event, which can directly or indirectly affect the Government's information technology supply chain. These threats are often undetected and in a manner that may result in significant risk to the end user. In addition, systems and components that span the Government's information technology supply chain infrastructure are accessed by a variety of individuals within an organization, supplier, or external service provider. The many access points increase the vulnerability and susceptibility of information exposure within the supply chain.

Further, information technology supply chain risks may include counterfeits, tampering, theft, and insertion of malicious software and hardware as well as poor manufacturing and development practices. NIST Special Publication 800-161 states that these risks are associated with an organization's decreased visibility into, understanding of, and control over how the technology it acquires is "developed, integrated, and deployed as well as the processes, procedures, and practices used to assure the integrity, security, resilience, and quality of the products and services." Threats and vulnerabilities created by malicious actors (*e.g.*, individuals, organizations, or nation states) are often sophisticated and difficult to detect, exposing an organization to significant risks.

Information technology supply chain risk management (SCRM) is the process of identifying, assessing, and mitigating the risks associated with the global and distributed nature of information technology product and service supply chains. The Federal Government currently uses varied and not-yet-standardized foundational practices, which make it difficult to consistently measure and manage information technology supply chain risks. According to NIST Special Publication 800-161, foundational practices include:

- Ensuring that organizations understand the cost and scheduling constraints of implementing information technology SCRM.

[1] See Appendix III for a glossary of terms.

[2] Dated April 2015.

- Integrating information security requirements into the acquisition process.
- Using applicable baseline security controls as one of the sources for security requirements.
- Ensuring a robust software quality control process.
- Establishing multiple sources (*e.g.*, delivery routes) for critical system elements.

Supply chain vulnerability is not a new problem. In December 2015, Juniper Networks revealed that it inadvertently delivered software updates containing malicious code. Researchers discovered that Juniper Networks had been using a National Security Agency–designed encryption algorithm that hackers had modified, creating a backdoor to its software. For approximately three years, a sophisticated adversary, possibly a foreign nation state, likely used this backdoor to decrypt communications to and from the many organizations using the software.

In July 2016, the Office of Management and Budget issued Circular No. A-130, *Management Information as a Strategic Resource*, that requires Federal agencies to analyze supply chain risks associated with potential contractors and their information technology products and services; implement SCRM principles to protect against the insertion of counterfeits, unauthorized production, tampering, theft, and insertion of malicious software as well as poor manufacturing and development practices throughout the system development life cycle; and develop SCRM plans to ensure the integrity, security, resilience, and quality of information systems.

Congress subsequently passed the Federal Acquisition Supply Chain Security Act of 2018,[3] requiring Federal agencies to develop an overall SCRM strategy and implementation plan as well as policies and processes to guide and govern SCRM activities. As supply chain threats are identified, Congress has added language in the National Defense Authorization Acts of 2018[4] and 2019[5] prohibiting the Federal Government from using products and services developed or provided by Kaspersky™ Lab as well as procuring or using certain "covered telecommunication equipment or services" that are produced by Huawei, ZTE, Hytera, Hikvision, and Dahua and their subsidiaries.

In December 2020, a significant hacking campaign was identified that the Government reported was likely orchestrated by a foreign nation state. Software from the SolarWinds® Corporation was breached giving hackers access to thousands of Government agency and private company systems using this software. The hackers were able to broadly distribute malware via a security update that acted as a Trojan horse. Cybersecurity experts have reported that it could take months to years to identify all the compromised systems.

Along with Congress, the President has expressed significant interest in and has taken steps to further limit the Government's exposure to supply chain risks. For example, the President signed

[3] Pub. L. No. 115-390, Title II, §§ 201-203, 132 Stat. 5173, 5178-5193 (codified at 41 U.S.C. § 1321 et seq.)(2018). Note: Federal Acquisition Supply Chain Security Act of 2018 is located in Title II of the Strengthening and Enhancing Cyber-Capabilities by Utilizing Risk Exposure Technology Act (SECURE Technology Act), Pub. L. No. 115-390, 132 Stat. 5173 (2018).

[4] National Defense Authorization Act for Fiscal Year 2018, Pub. L. No. 115-91, Title XVI, § 1634, 131 Stat. 1283, 1739-41 (2017).

[5] John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, Title VII, Subtitle H, § 889, 132 Stat. 1636, 1917-19 (2018).

Executive Order 14107, *America's Supply Chains*,[6] that directs Federal agencies to take a "whole-of-government" approach to assessing vulnerabilities in, and strengthening the resilience of, critical supply chains.

In addition, Federal agencies are now being assessed on their efforts to address supply chain risk exposure. For example, in a collaborative effort, the Office of Management and Budget, the Department of Homeland Security, and the Council of the Inspectors General on Integrity and Efficiency developed the *Fiscal Year 2021 Inspector General FISMA [Federal Information Security Modernization Act of 2014]*[7] *Reporting Metrics*. The reporting metrics are used to assess the effectiveness of a Federal agency's information security programs based on a maturity model spectrum in which the metrics ensure that agencies develop sound policies and procedures, and the advanced levels capture the extent that agencies institute those policies and procedures. For Fiscal Year 2021, a SCRM category was added to the reporting metrics focusing on the maturity of an agency's SCRM strategies, plans, policies, procedures, and processes to ensure that products, systems, system components, and services of external providers are consistent with the organization's cybersecurity and SCRM requirements.[8] In order to mitigate future attacks, it is imperative that processes and controls are in place to prevent and detect supply chain threats.

Results of Review

Initial Efforts Are Ongoing to Address Some Information Technology Supply Chain Risks

The Department of the Treasury (hereafter referred to as the Treasury Department) has overall responsibility for developing the strategy and guidance policies to manage information technology SCRM for the department and its bureaus. As of September 24, 2021, the Internal Revenue Service (IRS) stated that the Treasury Department is still finalizing the guidance policies as well as completing its internal reviews before they are shared with its bureaus for review and feedback. Once approved, the IRS plans to leverage the Treasury Department's guidance policies to create its own. As a result, the IRS is only in the beginning stages of information technology SCRM planning. However, the IRS has taken some preliminary steps to address information technology supply chain risks that include the following.

While the Treasury Department has overall responsibility for SCRM, initial IRS efforts are ongoing to address information technology supply chain risks.

- The Information Technology organization's Cybersecurity function has conducted some initial research on the Internet for SCRM frameworks that are publicly available to understand what other Federal agencies, *i.e.*, the Department of Defense, the

[6] Exec. Order No. 14017, 86 Fed. Reg. 11,849 (Feb. 24, 2021).

[7] Pub. L. No. 113-283, 128 Stat. 3073.

[8] For Fiscal Year 2021, SCRM metrics were not considered in an agency's overall information security program maturity rating in order to provide the agency sufficient time to fully implement the new requirements and standards.

Department of Energy, the General Services Administration, and the National Aeronautics and Space Administration, are undertaking to address information technology supply chain risks. For example, it has researched the Department of Defense's *Cybersecurity Maturity Model Certification* to better understand the certification process, its benefits, and how the IRS could leverage that model. The *Cybersecurity Maturity Model Certification* is used to help facilitate a vendor's implementation of cybersecurity best practices as well as to provide independent verification that the vendor has security controls and safeguards in place to protect sensitive data from disclosure or unauthorized use.

- Cybersecurity function personnel attended the *Software and Supply Chain Assurance Virtual Forums*, which are co-sponsored by the Department of Defense, the Department of Homeland Security, the General Services Administration, and NIST. The forums are held two to three times a year and provide a venue for government, industry, and academic participants from around the world to share their knowledge and expertise regarding software and supply chain risks; effective practices and mitigation strategies; tools and technologies; and any gaps related to the people, processes, or technologies involved.
- The Cybersecurity function has provided and expects to continue to provide input on the Treasury Department's planned information technology SCRM activities. The activities are worked at the department level with planned input from the bureaus and estimated completion by September 2022. For example, according to Cybersecurity function management, the Treasury Department is developing a questionnaire for vendors to complete and provide information technology supply chain information, such as known risks and security points of contact. The Treasury Department will also be collaborating with other Federal agencies and commercial entities as well as working with acquisition teams to enhance contractual language addressing supply chain risks prior to vendor selection and contract award.
- The IRS created a draft *Supply Chain Risk Management (SCRM) Strategy*, Version 0.1.[9] The strategy will provide a strategic roadmap for implementing effective information technology SCRM capabilities, practices, processes, and tools within the IRS in support of its vision, mission, and values. The strategy focuses on establishing a core foundational capability, such as defining policies, ownership, and dedicated resources to ensure that the IRS can expand and mature its information technology SCRM capabilities over time. The document further states that the strategy is dependent on the Treasury Department and industry-wide coordination efforts, processes, and decisions and will be updated as direction, guidance, and requirements are clarified and communicated.
- The IRS updated Internal Revenue Manual 10.8.1, *Information Technology (IT) Security, Policy and Guidance*,[10] based upon NIST Special Publication 800-53, *Security and Privacy Controls for Information Systems and Organizations*, Revision 5,[11] guidance. The

[9] Dated May 2021.

[10] Dated September 28, 2021.

[11] Dated September 2020.

updated manual includes a new set of security controls that the IRS must implement to help mitigate supply chain risks.

Although the IRS has taken some actions to address supply chain risks, continued reliance on weak SCRM controls could potentially compromise the confidentiality, integrity, and availability of the IRS's information systems as well as increase the risk of disruptions to its mission-critical functions.

Additional Steps Could Be Taken in the Short Term to Better Manage and Mitigate Information Technology Supply Chain Risks

The IRS has not implemented any security controls that would help mitigate information technology supply chain risks. The absence of information technology SCRM security controls increases the risk for disruptions to the IRS's operations and to meet its mission of helping taxpayers comply with their tax responsibilities and enforcing the tax laws with integrity and fairness to all. The IRS is waiting for the Treasury Department to finalize its guidance policies and all documents related to the planned information technology SCRM activities. While waiting on final guidance, the IRS could take additional steps to better manage and mitigate some information technology supply chain risks in the short term.

The IRS could take additional steps to mitigate some information technology supply chain risks and reduce the risk of operation disruptions.

NIST Special Publication 800-161 provides a number of security controls and security enhancements related to information technology SCRM that the IRS could immediately implement. For example, the IRS could increase organizational awareness by providing training regarding processes and controls that can help mitigate information technology supply chain risks. In addition, as part of its information security program planning, the IRS could begin documenting relevant SCRM controls and integrating them into ongoing security assessment and authorization activities.

Cybersecurity function management stated that NIST special publications, other than Special Publication 800-53, are not required to be part of the IRS's baseline of security controls, per Office of Management and Budget and NIST guidance. In addition, Cybersecurity function management stated that NIST special publications are implementation guides and standards and that agencies have latitude in how the special publications are used as well as how the security controls are implemented. However, while the IRS has discretion on how and whether security controls are implemented, we believe that, due to the severe nature of supply chain risks, it should have voluntarily implemented some of the SCRM security controls when NIST Special Publication 800-161 was first published. This would have proactively put the IRS in a better information technology SCRM posture. At the end of our audit work, the IRS updated Internal Revenue Manual 10.8.1 to include a set of SCRM security controls as well as references to NIST Special Publication 800-161.

In addition, we identified further steps that the IRS could take in the short term that will help improve its current information technology SCRM posture. We reached out to personnel and management from the Department of Defense, the Department of Energy, and the General Services Administration regarding their efforts in information technology SCRM. They provided the following examples implemented at their respective agencies that might help the IRS mitigate some supply chain risks while awaiting the final Treasury Department guidance.

- The Department of Defense developed contractual language that requires constant evaluation of the supply chain to eliminate risks as they are identified.
- The Department of Energy established a risk-based approach to conduct greater diligence on higher risk vendors.
- The General Services Administration, which maintains the Federal Acquisition Regulation, shared contractual language that requires vendors to provide a SCRM plan detailing how they will address counterfeit and illegally modified products as well as how they will reduce and mitigate information technology supply chain risks, where applicable.

At the end of our audit work, the IRS reached out to the Social Security Administration regarding its best practices to better manage supply chain risks. Personnel from the Social Security Administration provided contractual language they use for solicitations and awards that are subject to supply chain risk assessments.

Recommendation 1: The Chief Information Officer should implement controls to manage information technology supply chain risks based on the revised Internal Revenue Manual 10.8.1 guidance as well as do more to identify and incorporate SCRM best practices of other Federal agencies that would be applicable to the IRS.

> **Management's Response:** The IRS agreed with this recommendation. The Information Technology organization will implement controls to manage information technology supply chain risks based on the revised Internal Revenue Manual 10.8.1 guidance as well as do more to identify and incorporate SCRM best practices of other Federal agencies that would be applicable to the IRS.

Contract Clauses Are Not Consistently Applied to Protect Information Technology Procurements From Supply Chain Risks

The IRS is not reducing its risk exposure when procuring information technology because contracts do not consistently include clauses intended to manage supply chain risks. Personnel from the Office of the Chief Procurement Officer provided a list of 14 contract clauses to manage supply chain risks. Five of the clauses (*e.g.*, basic safeguarding of covered vendor information systems, prohibition on contracting for certain telecommunications, and video surveillance services or equipment) are from the Federal Acquisition Regulation[12] in response to new regulations enacted by the National Defense Authorization Act of 2019 and other laws. The remaining nine contract clauses (*e.g.*, notification of change in vendor personnel

The IRS can mitigate some information technology supply chain risks by consistently applying contract clauses.

[12] 48 C.F.R. § 52.204-21, *Basic Safeguarding of Covered Contractor Information Systems;* § 52.204-23, *Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities;* § 52.204-24, *Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment;* § 52.204-25, *Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment;* and § 52.204-26, *Covered Telecommunications Equipment or Services-Representation.*

employment status and submission of security forms and related materials) were created by the IRS and included in the *IRS Acquisition Policy, FY [Fiscal Year] 2021 edition*, Version 2.0,[13] in response to NIST, Treasury Department, and other guidance. However, while we recognize that not all contract clauses available for use may be applicable, we found that the use of contract clauses in similar procurement contracts[14] detailing vendor responsibilities to protect the IRS from information technology supply chain risks are not consistently applied.

We selected a judgmental sample[15] of 15 contracts procuring information technology products and services from a population of 114 Information Technology organization contracts signed between December 1, 2020, and March 31, 2021.[16] Twelve of the 14 potential contract clauses addressing supply chain risks were included in some, but not all six, of the contracts procuring software support and maintenance in our sample. Similarly, seven of the 14 potential contract clauses addressing supply chain risks were included in some, but not all four, of the contracts procuring comparable services to support application development activities.

In addition, contrary to expectations, we identified one contract procuring [redacted] products that included nine of the 14 potential contract clauses addressing supply chain risks, including references to safeguards against unauthorized disclosure of sensitive but unclassified information and references to not using any hardware, software, or service developed by Kaspersky Lab. When solely procuring [redacted] products, we do not see the relevance or application of including these clauses in the contract.[17]

We surveyed the contracting officers who signed the contracts in our sample to determine the reasons why they did or did not include the 14 contract clauses addressing supply chain risks in their respective contracts as well as to determine whether they were notified of or provided training on the new contract clauses. We identified 12 contracting officers for the 15 contracts in our sample that we selected for review. Of the 11 contracting officers that we surveyed,[18] they all responded that they use the mandatory contract clause building tool, DocScout, which provides suggested clauses for application in the contract, but inclusion of the contract clauses is left to their determination. Some contracting officers also responded that they only included the contract clauses because contracting policy required it. In addition, contracting officers responded that they are generally notified of new contract clauses by e-mail, which provides details on the policy updates from the Office of the Chief Procurement Officer.

According to management from the Office of the Chief Procurement Officer, notification of new contract clauses and policy updates are distributed by e-mail from the Office of Procurement's Policy Division. Management also stated that within the division, the Policy and Procedures section updates its Policy, Guidance, and Instructions biannually as well as conducts

[13] Dated June 30, 2021.

[14] Our review of contracts included their respective modifications, where applicable, because some contracts were created from a Government-wide acquisition contract, which were awarded prior to the required use of some of the supply chain procurement contract clauses. In these cases, the modifications subsequently included some of the required procurement contract clauses after the initial contract was awarded.

[15] A judgmental sample is a nonprobability sample, the results of which cannot be used to project to the population.

[16] The last enacted or requirement date for the use of the 14 contract clauses was November 2020. We selected contracts signed after that date for review to ensure the clauses' potential inclusion in the contracts.

[17] The remaining four contracts did not procure similar types of information technology products or services. As a result, we were unable to make an association with other contracts to complete our analysis on contract clause usage.

[18] One contracting officer had left the IRS.

informational training sessions to inform personnel of the updates and answer questions. In addition, management stated that the use and applicability of the clauses may vary based upon the requirements of each contract. Further, management stated that contracting officers are not trained on specific clauses, but they are provided opportunities to take training on Federal Acquisition Regulation updates through the Treasury Acquisition Institute as well as attend other internal training and lunch and learn information sessions.

The results of our survey with the contracting officers confirmed the inconsistent use and application of the contract clauses intended to manage supply chain risks. In addition, there is insufficient management oversight and no quality review process to ensure that contract clauses addressing supply chain risks are consistently used and included in contracts when procuring similar information technology products and services. While the IRS has a quality assurance process, IRS Procedure, Guidance, and Information 1004.71, *Review and Approval Procedures*,[19] does not require a review on the proper use and application of any specific contract clause.

The Chief Procurement Officer should:

Recommendation 2: Ensure that contracting officers are provided further instructions on the proper and consistent application of contract clauses addressing supply chain risks.

> **Management's Response:** The IRS agreed with this recommendation. The Office of the Chief Procurement Officer staff are notified of new contract clauses and policy updates by e-mail and provided with many opportunities for training and information sessions related to this each year. In Fiscal Year 2022, the Office of the Chief Procurement Officer staff and managers will be reminded about the proper and consistent application of contract clauses to include contract clauses addressing supply chain risks.

Recommendation 3: Ensure that the quality assurance process includes a review for the proper and consistent application of contract clauses addressing supply chain risks.

> **Management's Response:** The IRS agreed with this recommendation. The Office of Procurement Policy, Quality Assurance Section, will add the identified supply chain risk clauses to its Security and Privacy Clauses Checklist to verify that applicable clauses have been included in drafted solicitation documents and contracts before award.

[19] Dated June 30, 2021.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to evaluate the IRS's efforts to identify, assess, and mitigate information technology supply chain risks. To accomplish our objective, we:

- Reviewed Federal, Treasury Department, and IRS policies, procedures, and guidance; applicable best practices; and interim controls as well as interviewed Cybersecurity function personnel to determine whether the IRS is complying with supply chain risk guidelines.
- Interviewed Cybersecurity function personnel to determine the IRS's efforts in developing an information technology SCRM framework and implementing the *Department of the Treasury Cyber Supply Chain Risk Management* activities as well as identifying, assessing, and mitigating future supply chain risks.
- Interviewed personnel and management from the Department of Defense, the Department of Energy, and the General Services Administration to identify their information technology SCRM frameworks as well as best practices and interim controls associated with their efforts in developing the framework.
- Selected and reviewed a judgmental sample[1] of 15 contracts that procured information technology products and services from a population of 114 Information Technology organization contracts signed between December 1, 2020, and May 31, 2021, to determine whether the Office of the Chief Procurement Officer complied with supply chain risk guidelines and the National Defense Authorization Act. We selected a judgmental sample because we did not plan to project the results to the population.
- Surveyed 11 contracting officers to determine their reasons for including or not including contract clauses in their respective contracts. We interviewed management from the Office of the Chief Procurement Officer to determine whether contracting officers were notified of or provided training on the new contract clauses.

Performance of This Review

This review was performed with information obtained from the Information Technology organization's Cybersecurity function and the Office of the Chief Procurement Officer located at the New Carrollton Federal Building in Lanham, Maryland, and IRS Headquarters in Washington, D.C., during the period March through October 2021. 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.

[1] A judgmental sample is a nonprobability sample, the results of which cannot be used to project to the population.

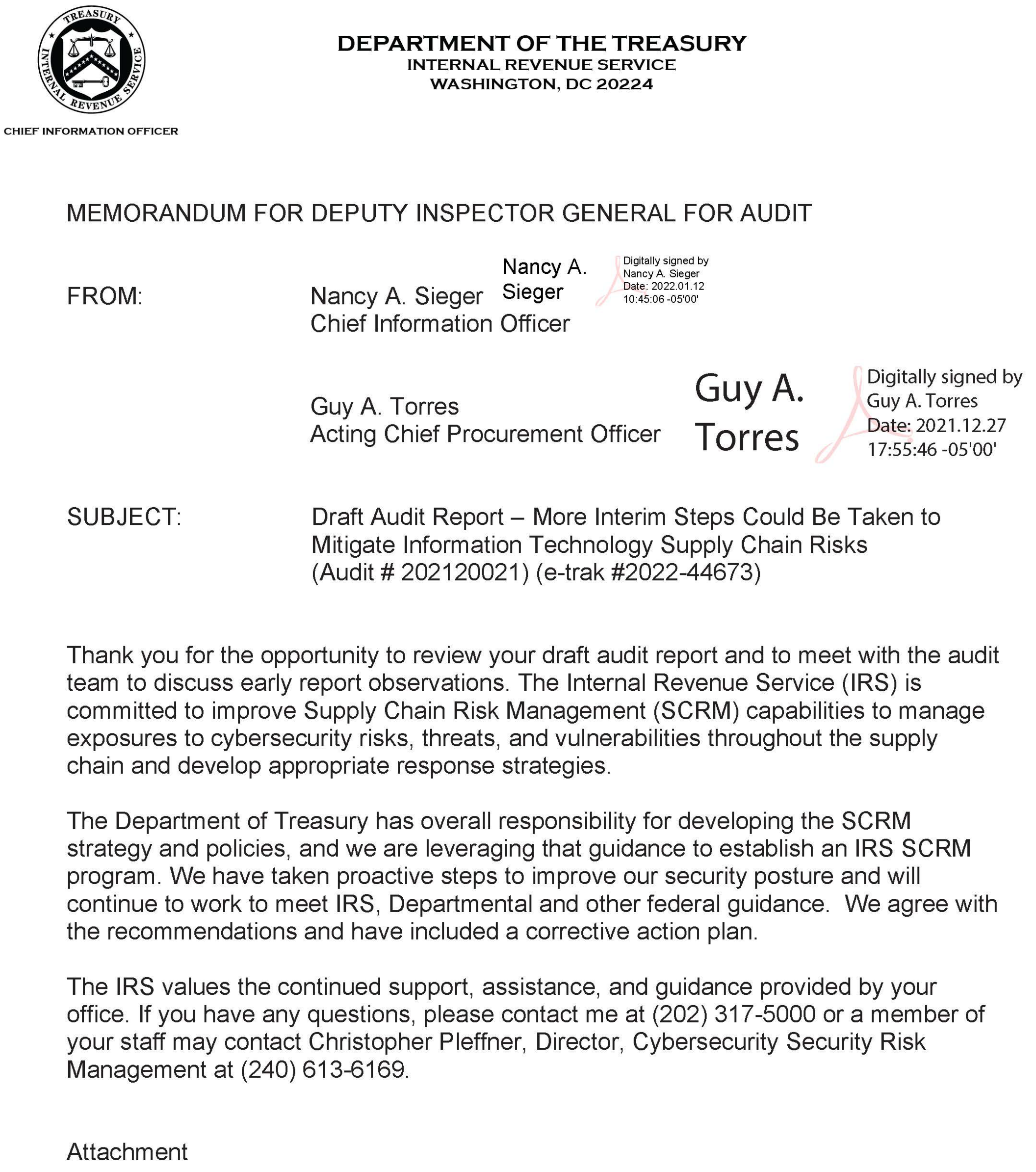
Major contributors to the report were Danny R. Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services); Bryce Kisler, Director; Louis Lee, Audit Manager; Jason Rosenberg, Lead Auditor; and Paula Benjamin-Grant, Auditor.

Internal Controls Methodology

Internal controls relate to management's plans, methods, and procedures used to meet their mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance. We determined that the following internal controls were relevant to our audit objective: Federal Acquisition Regulation and NIST guidance as well as various IRS policies and procedures related to information technology SCRM. We evaluated these controls by interviewing and surveying Information Technology organization and Office of the Chief Procurement Officer personnel concerning the implementation of information technology SCRM security controls as well as reviewing information technology procurement contracts and other relevant documents.

Appendix II

Management's Response to the Draft Report



CHIEF INFORMATION OFFICER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Nancy A. Sieger
Chief Information Officer

Nancy A. Sieger
Digitally signed by Nancy A. Sieger
Date: 2022.01.12 10:45:06 -05'00'

Guy A. Torres
Acting Chief Procurement Officer

Guy A. Torres
Digitally signed by Guy A. Torres
Date: 2021.12.27 17:55:46 -05'00'

SUBJECT: Draft Audit Report – More Interim Steps Could Be Taken to Mitigate Information Technology Supply Chain Risks (Audit # 202120021) (e-trak #2022-44673)

Thank you for the opportunity to review your draft audit report and to meet with the audit team to discuss early report observations. The Internal Revenue Service (IRS) is committed to improve Supply Chain Risk Management (SCRM) capabilities to manage exposures to cybersecurity risks, threats, and vulnerabilities throughout the supply chain and develop appropriate response strategies.

The Department of Treasury has overall responsibility for developing the SCRM strategy and policies, and we are leveraging that guidance to establish an IRS SCRM program. We have taken proactive steps to improve our security posture and will continue to work to meet IRS, Departmental and other federal guidance. We agree with the recommendations and have included a corrective action plan.

The IRS values the continued support, assistance, and guidance provided by your office. If you have any questions, please contact me at (202) 317-5000 or a member of your staff may contact Christopher Pleffner, Director, Cybersecurity Security Risk Management at (240) 613-6169.

Attachment

Attachment

Draft Audit Report – More Interim Steps Could Be Taken to Mitigate Information Technology Supply Chain Risk (Audit #202120021)

RECOMMENDATION 1:
The Chief Information Officer should implement controls to manage information technology supply chain risks based on the revised Internal Revenue Manual 10.8.1 guidance as well as do more to identify and incorporate SCRM best practices of other Federal agencies that would be applicable to the IRS.

CORRECTIVE ACTION #1:
The IRS agrees with this recommendation. IT will implement controls to manage information technology supply chain risks based on the revised Internal Revenue Manual 10.8.1 guidance as well as do more to identify and incorporate SCRM best practices of other Federal agencies that would be applicable to the IRS.

IMPLEMENTATION DATE:
February 15, 2023

RESPONSIBLE OFFICIALS:
Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN:
We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and review remediation progress monthly until completion.

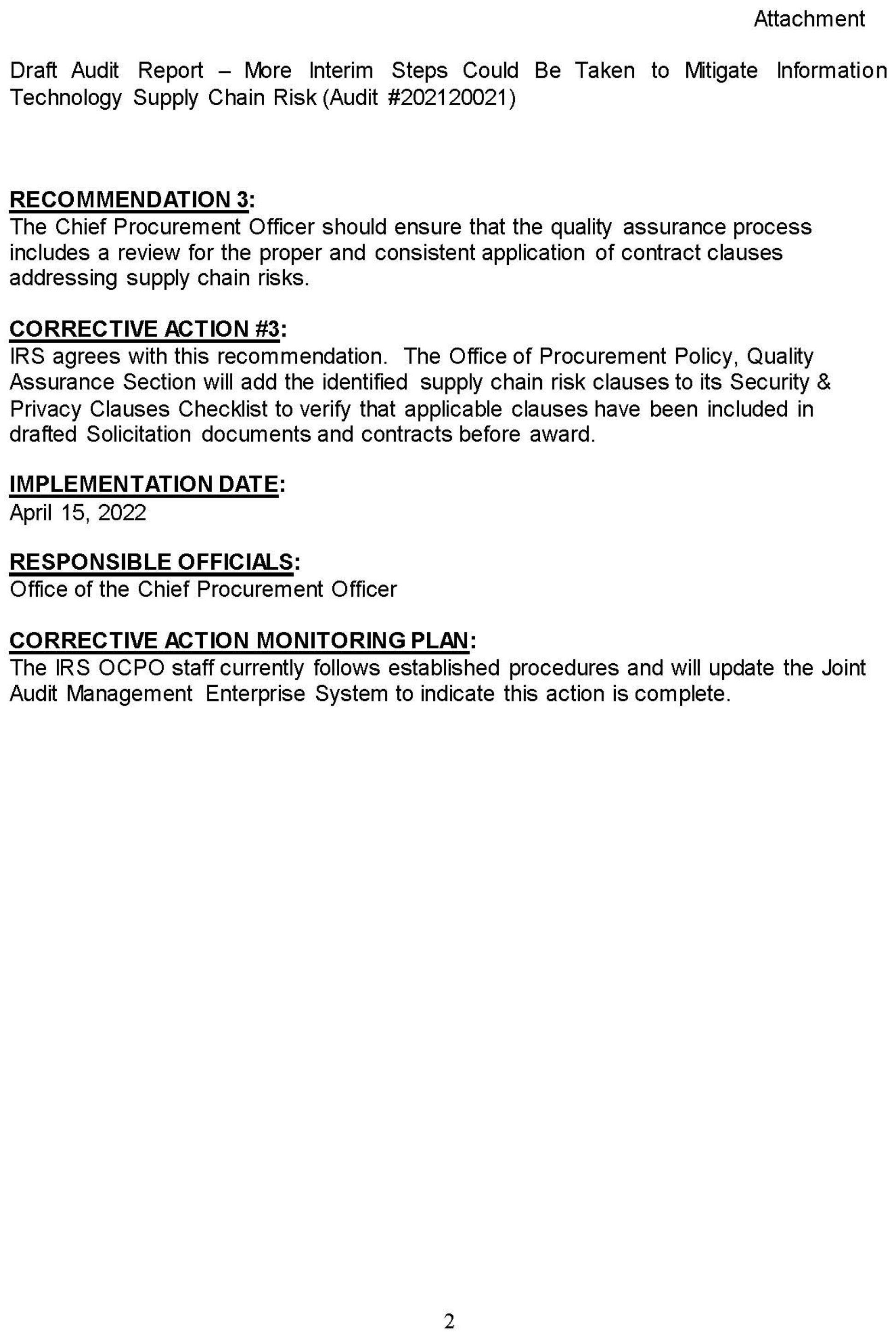
RECOMMENDATION 2:
The Chief Procurement Officer should ensure that contracting officers are provided further instructions on the proper and consistent application of contract clauses addressing supply chain risks.

CORRECTIVE ACTION #2:
IRS agrees with this recommendation. OCPO staff are notified of new contract clauses and policy updates by e-mail and provided with many opportunities for training and information sessions related to this each year. In Fiscal Year 2022, OCPO staff and managers will be reminded about the proper and consistent application of contract clauses to include contract clauses addressing supply chain risks.

IMPLEMENTATION DATE:
April 15, 2022

RESPONSIBLE OFFICIALS:
Office of the Chief Procurement Officer

CORRECTIVE ACTION MONITORING PLAN:
The IRS OCPO staff currently follows established procedures and will update the Joint Audit Management Enterprise System to indicate this action is complete.



Attachment

Draft Audit Report – More Interim Steps Could Be Taken to Mitigate Information Technology Supply Chain Risk (Audit #202120021)

RECOMMENDATION 3:
The Chief Procurement Officer should ensure that the quality assurance process includes a review for the proper and consistent application of contract clauses addressing supply chain risks.

CORRECTIVE ACTION #3:
IRS agrees with this recommendation. The Office of Procurement Policy, Quality Assurance Section will add the identified supply chain risk clauses to its Security & Privacy Clauses Checklist to verify that applicable clauses have been included in drafted Solicitation documents and contracts before award.

IMPLEMENTATION DATE:
April 15, 2022

RESPONSIBLE OFFICIALS:
Office of the Chief Procurement Officer

CORRECTIVE ACTION MONITORING PLAN:
The IRS OCPO staff currently follows established procedures and will update the Joint Audit Management Enterprise System to indicate this action is complete.

Appendix III

Glossary of Terms

Term	Definition
Algorithm	An ordered set of instructions applied to transform data input into processed data output, as a mathematical solution, descriptive statistics, Internet search engine result, or predictive text suggestions.
Contracting Officer	An agent of the Federal Government empowered to execute contracts and obligate Government funds.
Department of Defense	The department of the Federal Government charged with ensuring the military capacity of the United States is adequate to safeguard national security.
Department of Energy	The department of the Federal Government that sets forth and maintains the U.S. nuclear infrastructure and administers the country's energy policy.
Department of Homeland Security	The department of the Federal Government that works to improve the security of the United States. Its work includes customs, border, and immigration enforcement; emergency response to natural and manmade disasters; antiterrorism; and cybersecurity.
DocScout	A software application that inspects contracts to determine whether certain clauses belong, whether the clauses are up to date, and whether the clauses have been properly completed.
Federal Acquisition Regulation	The primary acquisition regulations for use by all Federal executive agencies in their acquisition of supplies and services with appropriated funds.
General Services Administration	An independent agency of the Federal Government, established to help manage and support the basic functioning of Federal agencies. It supplies products and services to Government offices, including real estate acquisition and facilities management.
Hacker	An unauthorized user who attempts to gain or gains access to an information system.
Information Technology	Any services, equipment, or interconnected system(s) or subsystem(s) of equipment that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an agency.
Kaspersky™ Lab	A company that develops and distributes information security software solutions to customers worldwide. It offers antimalware, cybersecurity intelligence software, and threat prevention products to protect information from viruses, spyware, ransomware, phishing, hackers, and spam.
Malicious Code	Software designed to infiltrate or damage a computer system without the owner's informed consent.

Malware	A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the computer's data, applications, or operating system.
National Aeronautics and Space Administration	An agency of the Federal Government created to oversee U.S. space exploration and aeronautics research. It is responsible for science and technology related to air and space.
National Defense Authorization Act	Legislation that Congress passes each year to make changes to the policies and organization of U.S. defense agencies and provide guidance on how military funding can be spent. In addition to the Department of Defense, the legislation also covers military-related programs run by other agencies, such as the Department of Energy's nuclear weapons programs and the Federal Bureau of Investigation's counterintelligence activities.
National Institute of Standards and Technology	A part of the Department of Commerce that is responsible for developing standards and guidelines to provide adequate information security for all Federal agency operations and assets.
National Security Agency	An agency of the Federal Government that coordinates and directs highly specialized activities to protect U.S. information systems and to produce foreign intelligence information.
Social Security Administration	An agency of the Federal Government that assigns Social Security Numbers and administers the Social Security retirement, survivors, and disability insurance programs.
System Integrator	An organization that provides customized services to the acquirer, including custom development, testing, operations, and maintenance.
Treasury Acquisition Institute	Established by the Treasury Department and the IRS, in partnership with the other Treasury bureaus, to coordinate and lead departmental and bureau efforts to obtain the best training for their acquisition professionals. It offers courses such as writing statements of work and contracting officer's representative training.
Trojan Horse	A computer program that appears to have a useful function but also has a hidden and potentially malicious function that evades security mechanisms.

Appendix IV

Abbreviations

IRS	Internal Revenue Service
NIST	National Institute of Standards and Technology
SCRM	Supply Chain Risk Management

**To report fraud, waste, or abuse,
call our toll-free hotline at:**

(800) 366-4484

By Web:

www.treasury.gov/tigta/

Or Write:

Treasury Inspector General for Tax Administration
P.O. Box 589
Ben Franklin Station
Washington, D.C. 20044-0589

Information you provide is confidential, and you may remain anonymous.