Calendar No. 666

115TH CONGRESS *2d Session*	SENATE	REPORT 115–408

FEDERAL ACQUISITION SUPPLY CHAIN SECURITY ACT OF 2018

R E P O R T

OF THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

TO ACCOMPANY

S. 3085

TO ESTABLISH A FEDERAL ACQUISITION SECURITY COUNCIL AND TO PROVIDE EXECUTIVE AGENCIES WITH AUTHORITIES RELATING TO MITIGATING SUPPLY CHAIN RISKS IN THE PROCUREMENT OF INFORMATION TECHNOLOGY, AND FOR OTHER PURPOSES

DECEMBER 4, 2018.—Ordered to be printed

U.S. GOVERNMENT PUBLISHING OFFICE
89–010 WASHINGTON : 2018

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

RON JOHNSON, Wisconsin, *Chairman*

ROB PORTMAN, Ohio
RAND PAUL, Kentucky
JAMES LANKFORD, Oklahoma
MICHAEL B. ENZI, Wyoming
JOHN HOEVEN, North Dakota
STEVE DAINES, Montana
JON KYL, Arizona

CLAIRE MCCASKILL, Missouri
THOMAS R. CARPER, Delaware
HEIDI HEITKAMP, North Dakota
GARY C. PETERS, Michigan
MAGGIE HASSAN, New Hampshire
KAMALA D. HARRIS, California
DOUG JONES, Alabama

CHRISTOPHER R. HIXON, *Staff Director*
GABRIELLE D'ADAMO SINGER, *Chief Counsel*
ELLIOTT A. WALDEN, *Counsel*
MARGARET E. DAUM, *Minority Staff Director*
CHARLES A. MOSKOWITZ, *Minority Senior Legislative Counsel*
JULIE G. KLEIN, *Minority Professional Staff Member*
LAURA W. KILBRIDE, *Chief Clerk*

Calendar No. 666

115TH CONGRESS, *2d Session* | SENATE | REPORT 115–408

FEDERAL ACQUISITION SUPPLY CHAIN SECURITY ACT OF 2018

DECEMBER 4, 2018.—Ordered to be printed

Mr. JOHNSON, from the Committee on Homeland Security and Governmental Affairs, submitted the following

R E P O R T

[To accompany S. 3085]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security and Governmental Affairs, to which was referred the bill (S. 3085) to establish a Federal Acquisition Security Council and to provide executive agencies with authorities relating to mitigating supply chain risks in the procurement of information technology, and for other purposes, having considered the same, reports favorably thereon with an amendment in the nature of a substitute and recommends that the bill, as amended, do pass.

CONTENTS

I. PURPOSE AND SUMMARY

S. 3085, the Federal Acquisition Supply Chain Security Act of 2018, establishes a whole-of government approach to supply chain risk management by creating a council and providing executive agencies with the necessary authorities to effectively share information and mitigate supply chain risks when procuring information and communications technology (ICT). The bill establishes the

Federal Acquisition Security Council (Council), an inter-agency body headed by the Office of Management and Budget (OMB). The Council is tasked with several functions related to supply chain risk management (SCRM), including the development of protocols for assessing risk, a government-wide strategy, and the authority to recommend exclusion or removal orders to executive agencies. The bill gives the Secretary of the Department of Homeland Security (DHS), the Secretary of the Department of Defense (DoD), and the Director of National Intelligence (ODNI) plenary authority to issue exclusion and removal orders based upon the Council's recommendations. The bill details a limited judicial review process available to an aggrieved company wishing to challenge the DHS, DoD, or ODNI determination.

II. Background and the Need for Legislation

Hostile nation states and other bad actors are attempting to gain unprecedented access to sensitive and classified information via the Federal ICT supply chains.[1] Experts have noted that using the supply chain, ICT "products could be modified to (1) perform below expectations or fail, (2) facilitate state or corporate espionage, of (3) otherwise compromise the confidentiality, integrity, or availability of a federal information technology system."[2] Many of the technologies the Federal Government relies on for vital, daily functions either could be or already have been targeted by bad actors or hostile nation states.[3] The actors' motivations vary, but the effects are the same: a less secure America.[4]

---

[1] *See, e.g., Confirmation Hearing for William R. Evanina to be Director of the National Counterintelligence and Security Center: Hearing Before the S. Select Comm. on Intelligence,* 115th Cong. (2018) (statement for the record by William Evanina, Director of the National Counterintelligence and Security Center, stating, "The most critical CI threats cut across these threat actors: influence operations, critical infrastructure, supply chain, and traditional as well as economic espionage. . . . Advanced technology previously available mainly to leading nation-states is now increasingly available to a wide range of nation-state and non-state actors as well. For example, a growing set of threat actors are now capable of using cyber operations to remotely access traditional intelligence targets, as well as a broader set of U.S. targets including critical infrastructure and supply chain, often without attribution."), available at https://www.intelligence.senate.gov/sites/default/files/documents/os-revanina-051518.PDF.

[2] *Supply Chain Vulnerabilities from China in U.S. Federal Information and Communications Technology* (Apr. 2018), https://www.uscc.gov/sites/default/files/Research/Interos_Supply%20Chain%20Vulnerabilities%20from%20China%20in%20U.S.%20Federal%20ICT_final.pdf.

[3] *See Current and Projected National Security Threats to the United States: Hearing Before the S. Select Comm. on Intelligence,* 112th Cong. (2012) (unclassified statement for the record by Director James Clapper, Director of National Intelligence, stating the "highly complex vulnerabilities associated with the IT supply chain" are one of the "greatest strategic challenges regarding cyber threats."), *available at* https://www.dni.gov/files/documents/Newsroom/Testimonies/20120131_testimony_ata.pdf; Office of the U.S. Trade Representative, Executive Office of the President, *Findings of the Investigation Into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation Under Section 301 of the Trade Act of 1974* (Mar. 22, 2018), *available at* https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF.

[4] H. Permanent Select Comm. on Intelligence, Chairman Mike Rogers and Ranking Member C.A. Dutch Ruppersberger, *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE,* 112th Cong. (Oct. 8, 2012), *available at* https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf (stating, "Inserting malicious hardware or software implants into Chinese-manufactured telecommunications components and systems headed for U.S. customers could allow Beijing to shut down or degrade critical national security systems in a time of crisis or war. Malicious implants in the components of critical infrastructure, such as power grids or financial networks, would also be a tremendous weapon in China's arsenal. Malicious Chinese hardware or software implants would also be a potent espionage tool for penetrating sensitive U.S. national security systems, as well as providing access to the closed American corporate networks that contain the sensitive trade secrets, advanced research and development data, and negotiating or litigation positions that China would find useful in obtaining an unfair diplomatic or commercial advantage over the United States. . . .").

This is not a new threat. The U.S. Intelligence Community (IC) and Congress have long warned that foreign governments may target the Federal ICT supply chain via certain products or services. This well-documented history includes:

• In 2011, the Office of National Counterintelligence Executive released a report stating, "Sensitive U.S. economic information and technology are targeted by the intelligence services, private sector companies, academic and research institutions, and citizens of dozens of countries."[5]

• In 2012, the U.S. House of Representatives' Permanent Select Committee on Intelligence (HPSCI) released a bipartisan report on the national security issues posed by Chinese telecommunications companies that stated in part, "[T]he U.S. government must pay particular attention to products produced by companies with ties to regimes that present the highest and most advanced espionage threats to the U.S., such as China."[6]

• In 2016, the U.S. Federal Bureau of Investigation (FBI) released a guide entitled, *Best Practices in Supply Chain Risk Management for the U.S. Government*, in which the FBI advises, among other things, to: "Identify the location of a service provider. If in a foreign country, identify potential relationships between the foreign government and the provider (suppliers, vendors, etc.). Identify the foreign country's laws or policies which enable it to request sensitive business information from the provider. Request the names, addresses, and roles of foreign individuals associated with, or who have access to the provider. . . . Identify if the provider employs foreign nationals . . . ."[7]

• In 2017, the DoD's Defense Science Board's Task Force on Cyber Supply Chain released a report stating that factors to consider when vetting a supplier could include ownership and control of the supplier.[8]

• In 2018, during testimony before the U.S. Senate Select Committee on Intelligence (SSCI), FBI Director Wray publicly stated: "I think probably the simplest way to put it in this setting would be that we're deeply concerned about the risks of allowing any company or entity that is beholden to foreign governments that don't share our values to gain positions of power inside our telecommunications networks. That provides the capacity to exert pressure or control over our telecommunications infrastructure. It provides the capacity to maliciously modify or steal information, and it provides the capacity to conduct undetected espionage. So, at a 100,000-foot

---

[5] Office of National Counterintelligence Executive, *Foreign Spies Stealing U.S. Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection & Industrial Espionage, 2009–2011* (Oct. 2011), *available at* https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/20111103_report_fecie.pdf.

[6] H. Permanent Select Comm. on Intelligence, Chairman Mike Rogers and Ranking Member C.A. Dutch Ruppersberger, *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE,* 112th Cong. (Oct. 8, 2012), *available at* https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf.

[7] U.S. Federal Bureau of Investigation, *Best Practices in Supply Chain Risk Management for the U.S. Government* (Feb. 2016), *available at* https://www.fbi.gov/file-repository/scrmbestpractices-1.pdf/view.

[8] Department of Defense, Defense Science Board Task Force on Cyber Supply Chain, *Final Report of the Defense Science Board Task Force on Cyber Supply Chain* (Feb. 2017), *available at* https://www.acq.osd.mil/dsb/reports/2010s/1028953.pdf.

level, at least in this setting, those are the kind of things that worry us."[9]

For years, the United States security agencies have understood the threat to national security systems posed by ICT supply chains, while grappling with how to appropriately share classified information and address the risk for all government agencies. The need for this legislation is underscored by several recent examples of supply chain risks discovered within the Federal ICT system.

AO Kaspersky Lab

AO Kaspersky Lab ("Kaspersky"), including its related entities such as Kaspersky Lab, Inc., is a cybersecurity and anti-virus software provider headquartered in Moscow, Russia.[10] Anti-virus software, by its very nature, is designed to have access to all files on the system on which it is running. Although the exact nature of how Kaspersky software operates is outside the scope of this report, Kaspersky's potential capabilities and the impacts on U.S. national security have been widely reported by a variety of leading security specialists and scholars.[11] In September 2017, DHS issued a Binding Operational Directive (BOD) ordering all Federal civilian executive agencies to identify and remove Kaspersky-branded products from Federal information systems.[12] This was the first time since receiving the authority under the Federal Information Security Modernization Act of 2014 to issue BODs that DHS used the authority to remove a product from the Federal supply chain.

Then-Acting Secretary of DHS Elaine Duke released the following statement contemporaneous with the BOD explaining why the Department acted. The statement said, in part:

> This action is based on the information security risks presented by the use of Kaspersky products on federal information systems. Kaspersky anti-virus products and solutions provide broad access to files and elevated privileges on the computers on which the software is installed, which can be exploited by malicious cyber actors to compromise those information systems. The Department is concerned about the ties between certain Kaspersky officials and Russian intelligence and other government agencies, and requirements under Russian law that allow Russian intelligence agencies to request or compel assistance from Kaspersky and to intercept communications transiting

[9] *Worldwide Threats: Hearing Before the S. Select Comm. on Intelligence,* 115th Cong. (2018) (statement of Director Chris Wray, Director of the U.S. Federal Bureau of Investigation).

[10] *Contact Us,* Kaspersky.com, https://usa.kaspersky.com/about/contact (last visited Oct. 17, 2018).

[11] *See, e.g.*, Herb Lin, *The Real Threat from Kaspersky Security Software,* Lawfare (Oct. 12, 2017), https://www.lawfareblog.com/real-threat-kaspersky-security-software (stating, "Of more concern to me is the idea that Kaspersky software has the capability to inspect the media ofµanyµcomputer running it for interesting files and to forward such files to Russian intelligence.") (emphasis in original); Nicholas Weaver, On Kaspersky, Lawfare (July 25, 2017), https://www.lawfareblog.com/kaspersky (noting that there is a risk of a "government-mandated malicious update."); see also Defendant's Motion to Dismiss, *Kaspersky Lab, Inc.; and Kaspersky Labs Limited v. United States of America,* D.D.C. (Mar. 26, 2018), Civ. No. 18–325 (CKK), *available at* https://www.nextgov.com/media/gbc/docs/pdfs_edit/032718kaspersky1ng.pdf.

[12] Department of Homeland Security, BOD–17–01: Removal of Kaspersky-Branded Products (Sept. 13, 2017), *available at* https://cyber.dhs.gov/assets/report/bod-17-01.pdf. BOD–17–01 defines "Kaspersky-branded products" as "information security products, solutions, and services supplied, directly or indirectly, by AO Kaspersky Lab or any of its predecessors, successors, parents, subsidiaries, or affiliates, including Kaspersky Lab North America, Kaspersky Lab, Inc., and Kaspersky Government Security Solutions, Inc. . . ."

> Russian networks. The risk that the Russian government, whether acting on its own or in collaboration with Kaspersky, could capitalize on access provided by Kaspersky products to compromise federal information and information systems directly implicates U.S. national security.[13]

In making the decision to issue the BOD, DHS consulted with multiple interagency partners.[14] Additionally, DHS offered Kaspersky the opportunity to submit a written response to address the Department's concerns and an opportunity to mitigate them.[15]

Congressional interest in Kaspersky continued throughout 2017.[16] In December 2017, Congress passed and the President signed into law the Fiscal Year 2018 National Defense Authorization Act (NDAA), which contained a statutory ban on Kaspersky products.[17] Unlike DHS' BOD, which applied only to Kaspersky branded products, the exclusion in the NDAA applied to "any hardware, software, or services developed or provided, in whole or in part, by Kaspersky Lab (or any successor entity); and any entity that controls, is controlled by, or is under common control with Kaspersky Lab; or any entity of which Kaspersky Lab has majority ownership."[18] The NDAA ban is much broader than the BOD as it targeted any product with Kaspersky coded embedded in it. Furthermore, this exclusion applied Government-wide. This provision went into effect on October 1, 2018.[19]

Kaspersky filed lawsuits challenging both the BOD and the NDAA exclusions.[20] Regarding the BOD challenge, Kaspersky argued that the directive violated the Administrative Procedures Act and the Due Process Clause of the Fifth Amendment.[21] The U.S. District Court for the District of Columbia found that Kaspersky lacked standing and granted the Government's motion to dismiss.[22] Kaspersky filed a separate lawsuit against the NDAA exclusion, arguing that the language in the NDAA constituted an unconstitutional bill of attainder.[23] The U.S. District Court for the District of Columbia held that the NDAA "does not inflict 'punishment' on Kaspersky Lab" under the definition of bill of attainder, again dis-

---

[13] Press Release, U.S. Department of Homeland Security, Acting Secretary Elaine Duke, DHS Statement on the Issuance of Binding Operational Directive 17–01 (Sept. 13, 2017), *available at* https://www.dhs.gov/news/2017/09/13/dhs-statement-issuance-binding-operational-directive-17-01.

[14] *Id.*

[15] *Id.*

[16] *See Disinformation: A Primer in Russian Active Measures and Influence Campaigns, Panel II: Hearing Before the S. Select Comm. on Intelligence*, 115th Cong. (2017) https://www.gpo.gov/fdsys/pkg/CHRG-115shrg25998/html/CHRG-115shrg25998.htm; *Bolstering the Government's Cybersecurity: Assessing the Risks of Kaspersky Lab Products to the Federal Government: Hearing Before the H. Comm. on Science, Space, and Technology*, 115th Cong. (2017), https://science.house.gov/legislation/hearings/bolstering-government-s-cybersecurity-assessing-risk-kaspersky-lab-products.

[17] NDAA 2018 § 1634.

[18] *Id.*

[19] *Id.*

[20] Memorandum Opinion, *Kaspersky Lab, Inc. et al.*, v. *U.S. Department of Homeland Security, et al.*, and *Kaspersky Lab, Inc. et al.*, v. *United States of America*, D.C.C. (May 30, 2018), *available at* https://cases.justia.com/federal/district-courts/district-of-columbia/dcdce/1:2017cv02697/192070/26/0.pdf?ts=1527759017.

[21] *Id.* at 3–5.

[22] *Id.*

[23] *Id.*

missing the case.[24] Kaspersky appealed the decision, and the appeal is still pending.[25]

Huawei Technologies Company and ZTE Corporation

Huawei Technologies Company ("Huawei") and ZTE Corporation ("ZTE") are telecommunications equipment manufacturers headquartered in Shenzhen, China, and represent a significant market share in the global telecommunications sector.[26] The presence of their products and services worldwide is prolific, including in the United States.[27] The United States Government has argued that Huawei and ZTE services and equipment may be used for nefarious or otherwise unauthorized purposes by the Chinese government.[28] During a hearing before SSCI, the Director of National Intelligence, Director of the Central Intelligence Agency, Director of the National Security Agency (NSA), Director of the Defense Intelligence Agency, Director of the FBI, and Director of the National Geospatial-Intelligence Agency were each asked if they would use products or services from Huawei or ZTE; all answered in the negative.[29]

The John S. McCain NDAA for Fiscal Year 2019, signed into law in August 2018, contained a provision banning the use of Huawei and ZTE from a "substantial or essential component of any system, or as critical technology as part of any system" within the Federal ICT supply chain.[30] The provision in the 2019 NDAA followed years of concern over the use of Huawei and ZTE products that culminated with several Federal agencies independently taking action to reassess the use of Huawei and ZTE products.[31]

S. 3085, the Federal Acquisition Supply Chain Security Act of 2018

The Committee continues to investigate threats to the Federal ICT supply chain and methods of mitigating the risk. The Kaspersky case made clear the potential threat to civilian agencies'

---

[24] *Id.*

[25] It is the policy of this Committee not to comment on matters currently before the courts. For details regarding the latest in litigation, *see generally* Joseph Marks, *Kaspersky Faces Tough Questions at Appeals Court*, Nextgov (Sept. 14, 2018), https://www.nextgov.com/cybersecurity/2018/09/kaspersky-faces-tough-questions-appeals-court/151282.

[26] *Company Profile: Huawei Technologies Co Ltd*, Bloomberg, https://www.bloomberg.com/profiles/companies/40978Z:CH-huawei-technologies-co-ltd (last visited Oct. 17, 2018); *Contact Us*, ZTE.com, https://www.zte.com.cn/global/about/contact-us (last visited Oct. 17, 2018).

[27] H. Permanent Select Comm. on Intelligence, Chairman Mike Rogers and Ranking Member C.A. Dutch Ruppersberger, *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE,* 112th Cong. (Oct. 8, 2012), *available at* https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf.

[28] *See generally, id.*; Office of the U.S. Trade Representative, Executive Office of the President, *Findings of the Investigation Into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation Under Section 301 of the Trade Act of 1974* (Mar. 22, 2018), available at https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF.

[29] *Worldwide Threats: Hearing Before the S. Select Comm. on Intelligence,* 115th Cong. (2018) (questioning by Senator Tom Cotton: "All the witnesses, I'd like to address this question to you. Would you please raise your hand if you would use products or services from Huawei or ZTE? None of you would. You obviously lead intelligence services, so that's something of a biased question. Raise your hand if you would recommend that private American citizens use Huawei or ZTE products or services. None of you again are raising your hand, thank you for that. . . .).

[30] NDAA 2019 § 889.

[31] *See* Stu Woo & Gordon Lubold, *Pentagon Orders Stores on Military Bases to Remove Huawei, ZTE Phones,* The Wall Street Journal (May 2, 2018), https://www.wsj.com/articles/pentagon-asking-military-bases-to-remove-huawei-zte-phones-1525262076; see also Federal Communications Commission, Notice of Proposed Rulemaking: WC Docket No. 18–89, Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs (Mar. 27, 2018), https://transition.fcc.gov/Daily_Releases/Daily_Business/2018/db0327/DOC-349937A1.pdf.

ICT purchases and systems. Since then, a number of disjointed efforts to address the supply chain risk from Government ICT purchases have emerged, but there is no cohesive framework for all agencies to follow. A whole of government approach is needed to give U.S. agencies the information and authorities they need to swiftly address ICT supply chain issues.

S. 3085 establishes the Federal Acquisition Security Council, chaired by OMB. This Council, comprised of civilian, DoD, and IC agencies, is designed to develop a government-wide strategy for addressing supply chain risks from ICT purchases, to facilitate information sharing among government agencies and to be the central, government-wide authority for SCRM activities. The composition of the Council allows for agencies with a critical stake in Federal SCRM to have a voice in the Government's policy direction. Among its various SCRM-related functions, the Council is required to identify and recommend the development of SCRM standards for executive agencies to use when addressing supply chain risks. This will provide uniformity in how agencies assess and address such risk. The Council must also identify or develop criteria for sharing information related to supply chain risk management, including information pertaining to the exercise of authorities under sections 1326 and 4713. This criteria is to include, among other things, the content to be shared, when sharing is mandated or voluntary, and when it is appropriate for an executive agency to rely on shared information to exercise its authorities under this bill. This is designed to prevent one or two executive agencies from being aware of a present supply chain risk and failing to notify other agencies of that risk. As such, another responsibility of the Council includes designating an appropriate executive agency to act as a "central hub" for receiving supply chain information submitted by other executive agencies. This will streamline the information-sharing process across the Federal Government.

Another authority granted to the Council is the ability to recommend exclusion or removal orders for "covered articles." Covered articles are items found in the ICT supply chain, including, but not limited to: IT, including cloud computing services; telecommunications equipment; hardware; and software. Once the Council issues a recommendation, the Secretary of DHS, the Defense Secretary, and the Director of National Intelligence are vested with plenary authority to act on those recommendations. Once one of those officials, or their delegates, have acted on the recommendation(s), the corresponding agencies and systems they are responsible for are required to abide by the order(s). In the event that the Secretary of DHS, Defense Secretary, and Director of National Intelligence all issue the same order(s), collectively resulting in a government-wide decision, the bill requires the Administrator of the General Services Administration (GSA) and officials at other agencies to effectuate the order(s) government-wide.

In the event the Council makes a recommendation, the bill requires the Council to provide notice of the recommendation to any named source. The notice must advise the source that: a recommendation has been made; the criteria the Council relied upon in making the recommendation, to the extent consistent with national security and law enforcement interests; that the source has 30 days after receipt of the notice to submit information and argu-

ments in opposition to the recommendation; of the procedures governing the review and possible issuance of an exclusion or removal order; and, if practicable and within the sole and unreviewable discretion of the Council, a description of any mitigation steps the source could take that may result in the Council rescinding its recommendation. If one of the authorized agency heads decides to act on the Council's recommendation and issues an exclusion or removal order, that official must notify any named source of the exclusion or removal order and of the information that formed the basis for the order, to the extent consistent with national security and law enforcement interests. These exclusion and removal orders require an annual review thereafter.

This legislation also authorizes the head of an executive agency to carry out a "covered procurement action" and to limit the disclosure of information relating to the basis for doing so. A covered procurement action includes: the exclusion of a source that fails to meet certain qualification requirements; the exclusion of a source that fails to achieve an acceptable rating for supply chain risk when evaluating contract award proposals; the determination that a source is not a responsible source; and the decision to withhold consent for a contractor to subcontract with a particular source or to direct a contractor to exclude a particular source. Except when addressing an urgent national security interest, an agency head may only carry out a covered procurement action after receiving a joint recommendation from their chief acquisition officer and the chief information officer, or officials performing similar functions if the agency does not have such officials, and after providing notice of the joint recommendation to any source named in the recommendation. This notice must advise the named source of the following information: that a recommendation is being considered or has been made; of the information that formed the basis for the recommendation, to the extent consistent with national security and law enforcement interests; that the source has 30 days to submit information and argument in opposition to the recommendation; and of the procedures governing the consideration of the submission and the possible exercise of the agency's authority.

Finally, this bill contains judicial review procedures that appropriately balance the need for aggrieved companies to receive due process with the need for the Federal Government to act swiftly to address threats, share sensitive and/or classified information, and ensure that information is protected from disclosure. Any action taken under section 1323 or 4713 is not subject to existing administrative review or judicial review procedures for government purchases, including bid protests before the Government Accountability Office or in any Federal court. The bill provides for the filing of petitions for judicial review only in the U.S. Court of Appeals for the D.C. Circuit. A petition must be filed within sixty days after a party is notified of an exclusion or removal order under section 1323 or a covered procurement action under section 4713, claiming that the action is unlawful. The court will consider such an action unlawful only if it finds it to be: arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law; contrary to constitutional right, power, privilege, or immunity; in excess of statutory jurisdiction; lacking substantial support in the administration record taken as a whole or in classified information submitted to

the court; or not in accord with procedures required by law. These constraints and the timeline of sixty days affords for an expeditious resolution. The U.S. Court of Appeals for the D.C. Circuit is granted exclusive jurisdiction over such claims, which is appropriate given its unique expertise with national security matters and handling of classified material.

III. Legislative History

Ranking Member Claire McCaskill (D–MO) introduced S. 3085, the Federal Acquisition Supply Chain Security Act of 2018, on June 19, 2018, with Senator James Lankford (R–OK). The bill was referred to the Committee on Homeland Security and Governmental Affairs.

The Committee considered S. 3085 at a business meeting on September 26, 2018. During the business meeting, Ranking Member McCaskill and Senator Lankford offered an amendment in the nature of a substitute that was twice modified to reflect discussions among Members of the Committee and feedback from relevant executive agencies. The bill, as amended by the McCaskill-Lankford Substitute Amendment as twice modified, was ordered reported favorably by voice vote en bloc. Senators present were Johnson, Portman, Lankford, Enzi, Hoeven, McCaskill, Carper, Heitkamp, Peters, Hassan, Harris, and Jones.

IV. Section-by-Section Analysis of the Bill, as Reported

Section 1. Short title

This section provides that the bill may be referred to as the "Federal Acquisition Supply Chain Security Act of 2018."

Sec. 2. Federal Acquisition Supply Chain Security.

Section 2 of the bill amends chapter 13 of title 41, United States Code (U.S.C.), by adding the following new subchapter at the end:

Subchapter III—Federal Acquisition Supply Chain Security

§ 1321. Definitions

This section defines or provides references for the following terms in the subchapter: "appropriate congressional committees and leadership;" "Council;" "covered article;" "covered procurement action;" "information and communications technology;" "intelligence community;" "national security system;" and "supply chain risk."

§ 1322. Federal Acquisition Security Council establishment and membership

This section establishes the Council, whose membership is comprised of the following agencies: OMB; GSA; DHS; ODNI, including the National Counterintelligence and Security Center; Department of Justice, including the FBI; DoD, including the NSA; Department of Commerce, including the National Institute of Standards and Technology (NIST); and any other executive agencies the Chairperson designates. Within 90 days of the bill's enactment, each agency represented on the Council is required to designate a lead representative who is an expert in SCRM, acquisitions, or information and communications technology. Each agency's lead represent-

ative is tasked with ensuring that their agency leadership and subject matter experts are kept apprised of the Council's business. The Director of OMB is required to designate a senior-level OMB official to serve as the Council's Chairperson. The Chairperson is tasked with several functions, including developing a charter for the Council. The Council is required to meet within 180 days after enactment and at least every quarter thereafter.

§ 1323. Functions and authorities

This section delineates the functions and authorities granted to the Council.

New subsection (a) outlines that the Council is required to perform several functions, including but not limited to: (1) recommending NIST to develop SCRM standards and practices for executive agencies; (2) developing criteria for sharing information regarding supply chain risk; (3) identifying an executive agency to act as a "clearing house" for several functions, including receiving supply chain risk information submitted by other executive agencies and facilitating the sharing of that information to support supply chain risk analyses; (4) identifying executive agencies to provide shared services and common contract solutions to support SCRM; (5) issuing guidance on any other steps necessary to address supply chain risks that may arise when executive agencies provide shared services, common contract solutions, acquisitions vehicles, or assisted acquisitions; and (6) engaging with the private sector and other nongovernmental stakeholders on SCRM in the acquisition process, as appropriate.

New subsection (b) states that, in its sole and unreviewable discretion, the Council may establish a program office and any other bodies it deems appropriate for the purpose of carrying out its functions.

New subsection (c) details the authority the Council has to issue exclusion or removal orders. The Council is required to establish criteria and procedures for several actions, including for: (1) recommending orders for executive agencies requiring the exclusion of sources or covered articles from executive agencies procurement actions, also known as "exclusion orders;" (2) recommending orders for executive agencies requiring the removal of covered articles from executive agency information systems, also known as "removal orders;" (3) requesting and approving exceptions to issued exclusion or removal orders; and (4) ensuring that any recommended orders do not conflict with standards issued under section 11331 of title 40 and that the Director of NIST is consulted with regarding any orders that would implement standards developed by NIST. Using these established criteria, the Council will make recommendations regarding the exclusion of sources or covered articles from any executive agency procurement action or the removal of covered articles from executive agency information systems. Recommendations must include several important components, including, but not limited to, information regarding the scope and applicability of the recommended exclusion or removal order and a summary of any risk assessment reviewed or made in support of the order.

New subsection (c) also states that the Council is required to issue a notice of its recommendation to any source named in the

recommendation. This is intended to provide notice to the source that a recommendation has been made; of the criteria the Council relied on in making the recommendation; and that the source has 30 days after receipt of the notice to submit information and argument in opposition of the recommendation.

New subsection (c) also details how exclusion and removal order recommendations become operable. Exclusion and removal order recommendations issued by the Council will be reviewed by the Secretary of DHS, for orders applicable to civilian agencies, to the extent not covered by clause (ii) and (iii); by the Secretary of DoD, for orders applicable to the DoD and national security systems other than sensitive compartmented information systems; and the Director of National Intelligence, for orders applicable to the intelligence community and sensitive compartmented information. These officials have sole and unreviewable discretion to issue exclusion and removal orders based upon the Council's recommendations. If officials from DHS, DoD, and ODNI issue orders collectively resulting in a government-wide exclusion, the Administrator of GSA and officials at other agencies responsible for management of the Federal Supply Schedule and government-wide acquisition and multi-agency contracts must help facilitate implementation of the orders by removing the identified covered articles or sources from contracts. Exclusion and removal orders must be reviewed at least annually by the issuing officials. An authorized official from the relevant issuing agency may rescind exclusion and removal orders. Once such an order has been issued, the issuing official must provide notice to any source named in the order. The issuing official must also notify the appropriate congressional committees and the aforementioned agency selected to be the "clearing house" for such information. All executive agencies are required to comply with exclusion and removal orders.

New subsection (d) states that the Council may request any information from executive agencies it deems necessary to carry out its functions.

New subsection (e) states that the Council must consult and coordinate, as appropriate, with other relevant councils.

New subsection (f) states that nothing in this section limits the authority of the Office of Federal Procurement Policy to carry out its responsibilities.

§ 1324. Strategic plan

This section requires the Council to create a strategic plan for addressing supply chain risks posed by the acquisition of covered articles within 180 days of enactment. The necessary components of this plan include, but are not limited to: (1) an identification and promulgation of best practices for executive agencies to assess and mitigate supply chain risks; (2) an evaluation of the effect of implanting new policies or procedures on existing contracts; and (3) a plan for the identification and mitigation of supply chain risks from existing and prospective information and communications technology made available to executive agencies by other executive agencies. This plan is due to Congress within seven days after completion.

§ 1325. Annual report

The Chairperson of the Council is required to submit an annual report to Congress on the Council's activities before December 31 of each year.

§ 1326. Requirements for executive agencies

This section outlines the responsibilities of each executive agency head for SCRM, which include, but are not limited to: (1) assessing the supply chain risk posed by the acquisition of covered articles and either avoiding, mitigating, accepting, or transferring that risk; and (2) prioritizing such assessments based on the criticality of the mission or asset. This section also includes clarifications for interagency acquisitions and assisted acquisitions. For interagency acquisitions, in which one agency purchases supplies or services using another agency's contract, SCRM activities are the responsibility of the funding agency. For assisted acquisitions, in which an agency performs acquisition-related functions on behalf of another agency, it is required that the parties negotiate the assignment of responsibilities. The Secretary of DHS may assist executive agencies in conducting risk assessments and provide additional tools as necessary in support of such actions.

§ 1327. Judicial review procedures

This section outlines the judicial review procedures applicable to an action taken under § 1323 or § 4713 of this title. New subsection (a) clarifies that any action taken under either § 1323 or § 4713 is not reviewable, either by administrative review or judicial review, including bid protests before the Government Accountability Office or in any Federal court.

New subsection (b) describes the process for petitioning exclusion or removal orders. After a party has been notified of an exclusion or removal order under § 1323 or a covered procurement action under section § 4713, the party has 60 days to file a petition for judicial review in the United States Court of Appeals for the District of Columbia Circuit ("court"). The court will rule that a covered action taken under § 1323 or § 4713 is unlawful if it is: (1) arbitrary, capricious, and an abuse of discretion; (2) contrary to constitutional right, power, privilege, or immunity; (3) in excess of statutory jurisdiction, authority, or limitation, or short of statutory right; (4) lacking substantial support in the administrative record taken as a whole or in classified information submitted to the court; or (5) not in accordance with procedures required by law. The court has exclusive jurisdiction over claims arising under these sections against the U.S., any U.S. department or agency, or any component or official of any such department or agency, subject to review by the U.S. Supreme Court.

New subsection (b) also describes the contents and procedures for the administrative record, which will apply to the review of a petition. The U.S. is required to file an administrative record with the court, which consists of the information that the appropriate official relied on when taking an action under § 1323 or § 4713. Information that is both unclassified and non-privileged in the administrative record will be provided to the petitioner, with appropriate protections for any information that is privileged or confidential. The following information may be included in the administrative

record and will only be submitted to the court *ex parte* and *in camera*: (1) classified information; (2) sensitive security information; (3) privileged law enforcement information; (4) information obtained or derived from any activity authorized under the Foreign Intelligence Surveillance Act of 1978, with several exceptions; and (5) information subject to privilege or protections under any other provision of law. Any of the previously described information must remain under seal. The administrative record must be returned after the time to seek further review has ended or after further proceedings have concluded. Any determination made by the court under this subsection is the exclusive remedy. In this section, the term "classified information" not only has the meaning given the term in 1(a) of the Classified Information Procedures Act, but also includes any information that the government has determined to require protection for reasons of national security and any restricted data, as defined in section 11 of the Atomic Energy Act of 1954.

§ 1327. Termination

This section states that the subchapter terminates five years after the day of enactment. Amendments made by this section take effect 90 days after the day of enactment and apply to contracts that are awarded before, on, or after that date. The Federal Acquisition Security Council must prescribe an interim final rule to implement subchapter III of chapter 13 of title 41, U.S.C. within one year of enactment, and the Council must issue a final rule no later than one year after prescribing that interim final rule. If the Council does not issue a final rule in that time frame, the Council will be required to submit a report to Congress explaining why they failed to do so.

Sec. 3. Authorities of Executive Agencies relating to mitigating supply chain risks in the procurement of covered articles

Section 3 of the bill amends chapter 47 of title 41, U.S.C., by adding the following new section to the end:

§ 14713. Authorities relating to mitigating supply chain risks in the procurement of covered articles

New subsection (a) establishes that heads of executive agencies have the authority to carry out a covered procurement action and to limit the disclosure of information relating to their basis for doing so.

New subsection (b) provides that an agency head may carry out a covered procurement action, absent an urgent national security interest, only after (1) obtaining a joint recommendation from the agency's CIO and chief acquisition officer, or comparable officials; (2) providing notice of the joint recommendation to any source named in the joint recommendation; (3) making a written determination that the use of the authority is, among other things, necessary to protect national security by reducing supply chain risk; and (4) providing notice of the determination to Congress. Any named sources must be provided with a notice containing the following information: (1) that a recommendation is being considered or has been made; (2) what information formed the basis for the recommendation, to the extent consistent with national security interests; (3) that the source has 30 days after receipt to submit an

argument against the recommendation; and (4) what procedures govern the consideration of that submission.

New subsection (c) provides an exception for cases in which an agency head determines that an urgent national security interest necessitates the immediate exercise of the authority provided in new subsection (a). This exception allows agency heads to, among other things, temporarily delay sending notice to named sources; however, agency heads are required to comply with all of the requirements of new subsection (b) as soon as practicable after the urgency has passed.

New subsection (d) states that an agency head may not delegate these authorities to an official below the level one level below the Deputy Secretary or Principal Deputy Director, except that the Secretary of Defense may delegate authority for removal orders to the Commander of U.S. Cyber Command.

New subsection (e) states that if an agency head has made the decision to limit the disclosure of information relating to their basis for carrying out a covered procurement action, that official must notify the aforementioned agency identified as a "clearing house" for such SCRM-related information.

New subsection (f) requires agency heads to annually review any covered procurement actions.

New subsection (g) requires the Federal Acquisition Regulatory Council to prescribe any regulations necessary to implement this section.

New subsection (h) requires the head of each agency to submit a report to Congress, at least annually, summarizing the actions taken under this section.

New subsection (i) states that this section applies to the DoD, Coast Guard, and National Aeronautics and Space Administration, notwithstanding § 3101(c)(1)(A) of this title.

New subsection (j) provides that the authority provided under subsection (a) terminates in 5 years.

New subsection (k) defines the terms "appropriate congressional committees and leadership;" "covered article;" "covered procurement;" "covered procurement action;" "information and communications technology;" and "supply chain risk."

Sec. 4. Federal Information Security Modernization Act

New subsection (a) amends the Federal Information Security Modernization Act to provide references to several provisions in this bill and to add a new SCRM-related provision. That Act provides a government-wide framework for the oversight and security of non-national security Federal executive branch information security.

New subsection (b) contains a rule of construction, clarifying that nothing in this bill alters or impedes any authority or responsibility under § 3553 of title 44, U.S.C., which addresses the authorities and functions of the Director of OMB and Secretary of DHS under the Federal Information Security Modernization Act.

Sec. 5. Effective date

Section 5 states that this bill will take effect 90 days after enactment.

V. Evaluation of Regulatory Impact

Pursuant to the requirements of paragraph 11(b) of rule XXVI of the Standing Rules of the Senate, the Committee has considered the regulatory impact of this bill and determined that the bill will have no regulatory impact within the meaning of the rules. The Committee agrees with the Congressional Budget Office's statement that the bill contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act (UMRA) and would impose no costs on state, local, or tribal governments.

VI. Congressional Budget Office Cost Estimate

U.S. Congress,
Congressional Budget Office,
Washington, DC, November 28, 2018.

Hon. Ron Johnson, *Chairman,*
Committee on Homeland Security and Governmental Affairs,
U.S. Senate, Washington, DC.

Dear Mr. Chairman: The Congressional Budget Office has prepared the enclosed cost estimate for S. 3085, the Federal Acquisition Supply Chain Security Act of 2018.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Matthew Pickford, who can be reached at 226–2860.

Sincerely,

Keith Hall,
Director.

Enclosure,

S. 3085—Federal Acquisition Supply Chain Security Act of 2018

S. 3085 would create the Federal Acquisition Security Council, which would work to mitigate security risks that may arise from information technology (IT), telecommunications services, and other goods and services procured by the federal government. The council would consist of representatives from at least 11 departments and agencies and a representative from the Office of Management and Budget (OMB) would serve as chair of the council.

Under the bill, the council would look at the security of the entire supply chain for goods and services procured by the government including threats from terrorism, piracy, and theft in both the real world and cyber space. (The term supply chain refers to the total number of organizations, individuals, and processes involved in producing and selling something to a final user.) Primary responsibilities for the council would include:

- Developing criteria for assessing threats and vulnerabilities to the supply chain, and
- Issuing guidance on risks to the supply chain and how to address such risks.

Using information from OMB and based on the scope of the council's responsibilities, CBO estimates that when fully implemented the council would spend about $2 million annually; most of that would be for the cost of about 10 employees. CBO estimates that implementing S. 3085 would cost $10 million over the 2019–2023

period; any spending would be subject to the availability of appropriated funds.

S. 3085 also would allow agencies to change their procurement actions based on expected risks to the agency from different acquisitions. Those changes would involve preparing risk management plans and strategies to assess risks to the supply chain prior to purchasing and goods or services.

CBO is unaware of any comprehensive information on the security of the government's supply chain. CBO aims to produce estimates that generally reflect the middle of a range of most likely outcomes that would result if the legislation was enacted. However, CBO cannot determine how agencies currently handle supply chain risks nor how many resources are devoted to those activities. In addition, what policies, procedures, or guidance the new council would provide to agencies is not clear. Finally, under existing authority initially provided by section 806 of Public Law 111–383 and recently reauthorized by section 881 of the 2019 National Defense Authorization Act (P.L. 115–232), the Department of Defense can currently perform many of the activities described in section 3 of S. 3085. However, CBO cannot determine whether those authorities have ever been used. Thus, CBO cannot estimate whether implementing that section would have costs or savings for government agencies.

CBO expects that agencies would continue to procure goods and services at the lowest price available and that issues involving supply chain risk would not significantly increase or decrease the costs of goods and services procured by the government.

Enacting S. 3085 could affect direct spending by agencies that are authorized to use receipts from the sale of goods, fees, and other collections to cover operating costs. Therefore, pay-as-you-go procedures apply. Because most agencies can adjust the amounts collected as operating costs change, CBO estimates that any net changes in direct spending by those agencies would be negligible. Enacting the bill would not affect revenues.

CBO estimates that enacting S. 3085 would not increase net direct spending or on-budget deficits in any of the four consecutive 10-year periods beginning in 2029.

S. 3085 contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act.

The CBO staff contacts for this estimate are Matthew Pickford and Ray Hall. The estimate was reviewed by H. Samuel Papenfuss, Deputy Assistant Director for Budget Analysis.

VII. Changes in Existing Law Made by the Bill, as Reported

In compliance with paragraph 12 of rule XXVI of the Standing Rules of the Senate, changes in existing law made by the bill, as reported, are shown as follows: (existing law proposed to be omitted is enclosed in brackets, new matter is printed in italic, and existing law in which no change is proposed is shown in roman):

UNITED STATES CODE

* * * * * * *

TITLE 41—PUBLIC CONTRACTS

* * * * * * *

Subtitle I—Federal Procurement Policy

* * * * * * *

DIVISION B—OFFICE OF FEDERAL PROCUREMENT POLICY

* * * * * * *

CHAPTER 13—ACQUISITION COUNCILS

Subchapter I—Federal Acquisition Regulatory Council

Subchapter II—Chief Acquisition Officers Council

Subchapter III—Federal Acquisition Supply Chain Security

* * * * * * *

Subchapter II—Chief Acquisition Officers Council

* * * * * * *

Subchapter III—Federal Acquisition Supply Chain Security

SEC. 1321. DEFINITIONS.

In this subchapter:

(1) APPROPRIATE CONGRESSIONAL COMMITTEES AND LEADERSHIP.—The term "appropriate congressional committees and leadership" means—

(A) the Committee on Homeland Security and Governmental Affairs, the Committee on the Judiciary, the Committee on Armed Services, the Committee on Appropriations, the Select Committee on Intelligence, and the majority and minority leader of the Senate; and

(B) the Committee on Oversight and Government Reform, the Committee on the Judiciary, the Committee on Armed Services, the Committee on Appropriations, the Committee on Homeland Security, the Permanent Select Committee on

Intelligence, and the Speaker and minority leader of the House of Representatives.

(2) COUNCIL.—The term "Council" means the Federal Acquisition Security Council established under section 1322(a) of this title.

(3) COVERED ARTICLE.—The term "covered article" has the meaning given that term in section 4713 of this title.

(4) COVERED PROCUREMENT ACTION.—The term "covered procurement action" has the meaning given that term in section 4713 of this title.

(5) INFORMATION AND COMMUNICATIONS TECHNOLOGY.—The term "information and communications technology" has the meaning given that term in section 4713 of this title.

(6) INTELLIGENCE COMMUNITY.—The term "intelligence community" has the meaning given that term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)).

(7) NATIONAL SECURITY SYSTEM.—The term "national security system" has the meaning given that term in section 3552 of title 44.

(8) SUPPLY CHAIN RISK.—The term "supply chain risk" has the meaning given that term in section 4713 of this title.

SEC. 1322. FEDERAL ACQUISITION SECURITY COUNCIL ESTABLISHMENT AND MEMBERSHIP.

(a) ESTABLISHMENT.—There is established in the executive branch a Federal Acquisition Security Council.

(b) MEMBERSHIP.—

(1) IN GENERAL.—The following agencies shall be represented on the Council:

(A) The Office of Management and Budget.

(B) The General Services Administration.

(C) The Department of Homeland Security.

(D) The Office of the Director of National Intelligence, including the National Counterintelligence and Security Center.

(E) The Department of Justice, including the Federal Bureau of Investigation.

(F) The Department of Defense, including the National Security Agency.

(G) The Department of Commerce, including the National Institute of Standards and Technology.

(H) Such other executive agencies as determined by the Chairperson of the Council.

(2) LEAD REPRESENTATIVES.—

(A) DESIGNATION.—

(i) IN GENERAL.—Not later than 90 days after the date of the enactment of the Federal Acquisition Supply Chain Security Act of 2018, the head of each agency represented on the Council shall designate a representative of that agency as the lead representative on the Council.

(ii) REQUIREMENTS.—The representative of an agency designated under clause (i) shall have expertise in supply chain risk management, acquisitions, or information and communications technology.

(B) FUNCTIONS.—The lead representative of an agency designated under subparagraph (A) shall ensure that appropriate personnel, including leadership and subject matter experts of the agency, are aware of the business of the Council.

(c) CHAIRPERSON.—

(1) DESIGNATION.—Not later than 90 days after the date of the enactment of the Federal Acquisition Supply Chain Security Act of 2018, the Director of the Office of Management and Budget shall designate a senior-level official from the Office of Management and Budget to serve as the Chairperson of the Council.

(2) FUNCTIONS.—The Chairperson shall perform functions that include—

(A) subject to subsection (d), developing a schedule for meetings of the Council;

(B) designating executive agencies to be represented on the Council under subsection (b)(1)(H);

(C) in consultation with the lead representative of each agency represented on the Council, developing a charter for the Council; and

(D) not later than 7 days after completion of the charter, submitting the charter to the appropriate congressional committees and leadership.

(d) MEETINGS.—The Council shall meet not later than 180 days after the date of the enactment of the Federal Acquisition Supply Chain Security Act of 2018 and not less frequently than quarterly thereafter.

SEC. 1323. FUNCTIONS AND AUTHORITIES.

(a) IN GENERAL.—The Council shall perform functions that include the following:

(1) Identifying and recommending by the National Institute of Standards and Technology of supply chain risk management standards, guidelines, and practices for executive agencies to use when assessing and developing mitigation strategies to address supply chain risks, particularly in the acquisition and use of covered articles under section 1326(a) of this title.

(2) Identifying or developing criteria for sharing information with respect to supply chain risk, including information related to the exercise of authorities provided under this section and sections 1326 and 4713 of this title. At a minimum, such criteria shall address—

(A) the content to be shared;

(B) the circumstances under which sharing is mandated or voluntary; and

(C) the circumstances under which it is appropriate for an executive agency to rely on information made available through such sharing in exercising the responsibilities and authorities provided under this section and section 4713 of this title.

(3) Identifying an appropriate executive agency to—

(A) accept information submitted by executive agencies based on the criteria established under paragraph (2);

(B) facilitate the sharing of information received under subparagraph (A) to support supply chain risk analyses

under section 1326 of this title, recommendations under this section, and covered procurement actions under section 4713 of this title;

(C) share with the Council information regarding covered procurement actions by executive agencies taken under section 4713 of this title; and

(D) inform the Council of orders issued under this section.

(4) Identifying, as appropriate, executive agencies to provide—

(A) shared services, such as support for making risk assessments, validation of products that may be suitable for acquisition, and mitigation activities; and

(B) common contract solutions to support supply chain risk management activities, such as subscription services or machine-learning-enhanced analysis applications to support informed decision making.

(5) Identifying and issuing guidance on additional steps that may be necessary to address supply chain risks arising in the course of executive agencies providing shared services, common contract solutions, acquisitions vehicles, or assisted acquisitions.

(6) Engaging, as appropriate, with the private sector and other nongovernmental stakeholders on issues relating to the management of supply chain risks posed by the acquisition of covered articles.

(7) Carrying out such other actions, as determined by the Council, that are necessary to reduce the supply chain risks posed by acquisitions and use of covered articles.

(b) PROGRAM OFFICE AND COMMITTEES.—The Council may establish a program office and any committees, working groups, or other constituent bodies the Council deems appropriate, in its sole and unreviewable discretion, to carry out its functions.

(c) AUTHORITY FOR EXCLUSION OR REMOVAL ORDERS.—

(1) CRITERIA.—To reduce supply chain risk, the Council shall establish criteria and procedures for—

(A) recommending orders applicable to executive agencies requiring the exclusion of sources or covered articles from executive agency procurement actions (in this section referred to as 'exclusion orders');

(B) recommending orders applicable to executive agencies requiring the removal of covered articles from executive agency information systems (in this section referred to as removal orders');

(C) requesting and approving exceptions to an issued exclusion or removal order when warranted by circumstances, including alternative mitigation actions; and

(D) ensuring that recommended orders do not conflict with standards and guidelines issued under section 11331 of title 40 and that the Council consults with the Director of the National Institute of Standards and Technology regarding any recommended orders that would implement standards and guidelines developed by the National Institute of Standards and Technology.

(2) RECOMMENDATIONS.—The Council shall use the criteria established under paragraph (1), information made available

under subsection (a)(3), and any other information the Council determines appropriate to issue recommendations, for application to executive agencies or any subset thereof, regarding the exclusion of sources or covered articles from any executive agency procurement action, including source selection and consent for a contractor to subcontract, or the removal of covered articles from executive agency information systems. Such recommendations shall include—

(A) information necessary to positively identify the sources or covered articles recommended for exclusion or removal;

(B) information regarding the scope and applicability of the recommended exclusion or removal order;

(C) a summary of any risk assessment reviewed or conducted in support of the recommended exclusion or removal order;

(D) a summary of the basis for the recommendation, including a discussion of less intrusive measures that were considered and why such measures were not reasonably available to reduce supply chain risk;

(E) a description of the actions necessary to implement the recommended exclusion or removal order; and

(F) where practicable, in the Council's sole and unreviewable discretion, a description of mitigation steps that could be taken by the source that may result in the Council rescinding a recommendation.

(3) NOTICE OF RECOMMENDATION AND REVIEW.—A notice of the Council's recommendation under paragraph (2) shall be issued to any source named in the recommendation advising—

(A) that a recommendation has been made;

(B) of the criteria the Council relied upon under paragraph (1) and, to the extent consistent with national security and law enforcement interests, of information that forms the basis for the recommendation;

(C) that, within 30 days after receipt of notice, the source may submit information and argument in opposition to the recommendation;

(D) of the procedures governing the review and possible issuance of an exclusion or removal order pursuant to paragraph (4); and

(E) where practicable, in the Council's sole and unreviewable discretion, a description of mitigation steps that could be taken by the source that may result in the Council rescinding the recommendation.

(4) EXCLUSION AND REMOVAL ORDERS.—

(A) ORDER ISSUANCE.—Recommendations of the Council under paragraph (2), together with any information submitted by a source under paragraph (3) related to such a recommendation, shall be reviewed by the following officials, who in their sole and unreviewable discretion may issue exclusion and removal orders based upon such recommendations:

(i) The Secretary of Homeland Security, for exclusion and removal orders applicable to civilian agencies, to the extent not covered by clause (ii) or (iii).

(ii) The Secretary of Defense, for exclusion and removal orders applicable to the Department of Defense and national security systems other than sensitive compartmented information systems.

(iii) The Director of National Intelligence, for exclusion and removal orders applicable to the intelligence community and sensitive compartmented information systems, to the extent not covered by clause (ii).

(B) DELEGATION.—The officials identified in subparagraph (A) may not delegate any authority under this subparagraph to an official below the level one level below the Deputy Secretary or Principal Deputy Director, except that the Secretary of Defense may delegate authority for removal orders to the Commander of the United States Cyber Command, who may not re-delegate such authority to an official below the level one level below the Deputy Commander.

(C) FACILITATION OF EXCLUSION ORDERS.—If officials identified under this paragraph from the Department of Homeland Security, the Department of Defense, and the Office of the Director of National Intelligence issue orders collectively resulting in a governmentwide exclusion, the Administrator for General Services and officials at other executive agencies responsible for management of the Federal Supply Schedules, governmentwide acquisition contracts and multi-agency contracts shall help facilitate implementation of such orders by removing the covered articles or sources identified in the orders from such contracts.

(D) REVIEW OF EXCLUSION AND REMOVAL ORDERS.—The officials identified under this paragraph shall review all exclusion and removal orders issued under subparagraph (A) not less frequently than annually pursuant to procedures established by the Council.

(E) RESCISSION.—Orders issued pursuant to subparagraph (A) may be rescinded by an authorized official from the relevant issuing agency.

(5) NOTIFICATIONS.—Upon issuance of an exclusion or removal order pursuant to paragraph (4)(A), the official identified under that paragraph who issued the order shall—

(A) notify any source named in the order of—

(i) the exclusion or removal order; and

(ii) to the extent consistent with national security and law enforcement interests, information that forms the basis for the order;

(B) provide classified or unclassified notice of the exclusion or removal order to the appropriate congressional committees and leadership; and

(C) provide the exclusion or removal order to the agency identified in subsection (a)(3).

(6) COMPLIANCE.—Executive agencies shall comply with exclusion and removal orders issued pursuant to paragraph (4).

(d) AUTHORITY TO REQUEST INFORMATION.—The Council may request such information from executive agencies as is necessary for the Council to carry out its functions.

(e) RELATIONSHIP TO OTHER COUNCILS.—The Council shall consult and coordinate, as appropriate, with other relevant councils, in-

cluding the Chief Information Officers Council, the Chief Acquisition Officers Council, and the Federal Acquisition Regulatory Council, with respect to supply chain risks posed by the acquisition and use of covered articles.

(f) RULE OF CONSTRUCTION.—Nothing in this section shall limit the authority of the Office of Federal Procurement Policy to carry out the responsibilities of that Office under any other provision of law.

SEC. 1324. STRATEGIC PLAN.

(a) IN GENERAL.—Not later than 180 days after the date of the enactment of the Federal Acquisition Supply Chain Security Act of 2018, the Council shall develop a strategic plan for addressing supply chain risks posed by the acquisition of covered articles and for managing such risks that includes—

(1) the criteria and processes required under section 1323(a) of this title, including a threshold and requirements for sharing relevant information about such risks with all executive agencies;

(2) an identification of existing authorities for addressing such risks;

(3) an identification and promulgation of best practices and procedures and available resources for executive agencies to assess and mitigate such risks;

(4) recommendations for any legislative, regulatory, or other policy changes to improve efforts to address such risks;

(5) an evaluation of the effect of implementing new policies or procedures on existing contracts and the procurement process;

(6) a plan for engaging with executive agencies, the private sector, and other nongovernmental stakeholders to address such risks;

(7) a plan for identification, assessment, mitigation, and vetting of supply chain risks from existing and prospective information and communications technology made available by executive agencies to other executive agencies through common contract solutions, shared services, acquisition vehicles, or other assisted acquisition services; and

(8) plans to strengthen the capacity of all executive agencies to conduct assessments of—

(A) the supply chain risk posed by the acquisition of covered articles; and

(B) compliance with the requirements of this subchapter.

(b) SUBMISSION TO CONGRESS.—Not later than 7 calendar days after completion of the strategic plan required by subsection (a), the Chairperson of the Council shall submit the plan to the appropriate congressional committees and leadership.

SEC. 1325. ANNUAL REPORT.

Not later than December 31 of each year, the Chairperson of the Council shall submit to the appropriate congressional committees and leadership a report on the activities of the Council during the preceding 12-month period.

SEC. 1326. REQUIREMENTS FOR EXECUTIVE AGENCIES.

(a) IN GENERAL.—The head of each executive agency shall be responsible for—

(1) assessing the supply chain risk posed by the acquisition and use of covered articles and avoiding, mitigating, accepting, or transferring that risk, as appropriate and consistent with the standards, guidelines, and practices identified by the Council under section 1323(a)(1); and

(2) prioritizing supply chain risk assessments conducted under paragraph (1) based on the criticality of the mission, system, component, service, or asset.

(b) INCLUSIONS.—The responsibility for assessing supply chain risk described in subsection (a) includes—

(1) developing an overall supply chain risk management strategy and implementation plan and policies and processes to guide and govern supply chain risk management activities;

(2) integrating supply chain risk management practices throughout the life cycle of the system, component, service, or asset;

(3) limiting, avoiding, mitigating, accepting, or transferring any identified risk;

(4) sharing relevant information with other executive agencies as determined appropriate by the Council in a manner consistent with section 1323(a) of this title;

(5) reporting on progress and effectiveness of the agency's supply chain risk management consistent with guidance issued by the Office of Management and Budget and the Council; and

(6) ensuring that all relevant information, including classified information, with respect to acquisitions of covered articles that may pose a supply chain risk, consistent with section 1323(a) of this title, is incorporated into existing processes of the agency for conducting assessments described in subsection (a) and ongoing management of acquisition programs, including any identification, investigation, mitigation, or remediation needs.

(c) INTERAGENCY ACQUISITIONS.—

(1) IN GENERAL.—Except as provided in paragraph (2), in the case of an interagency acquisition, subsection (a) shall be carried out by the head of the executive agency whose funds are being used to procure the covered article.

(2) ASSISTED ACQUISITIONS.—In an assisted acquisition, the parties to the acquisition shall determine, as part of the interagency agreement governing the acquisition, which agency is responsible for carrying out subsection (a).

(3) DEFINITIONS.—In this subsection, the terms 'assisted acquisition' and 'interagency acquisition' have the meanings given those terms in section 2.101 of title 48, Code of Federal Regulations (or any corresponding similar regulation or ruling).

(d) ASSISTANCE.—The Secretary of Homeland Security may—

(1) assist executive agencies in conducting risk assessments described in subsection (a) and implementing mitigation requirements for information and communications technology; and

(2) provide such additional guidance or tools as are necessary to support actions taken by executive agencies.

SEC. 1327. JUDICIAL REVIEW PROCEDURES.

(a) IN GENERAL.—Except as provided in subsection (b) and chapter 71 of this title, and notwithstanding any other provision of law,

an action taken under section 1323 or 4713 of this title, or any action taken by an executive agency to implement such an action, shall not be subject to administrative review or judicial review, including bid protests before the Government Accountability Office or in any Federal court.

(b) PETITIONS.—

(1) IN GENERAL.—Not later than 60 days after a party is notified of an exclusion or removal order under section 1323(c)(5) of this title or a covered procurement action under section 4713 of this title, the party may file a petition for judicial review in the United States Court of Appeals for the District of Columbia Circuit claiming that the issuance of an exclusion or removal order or covered procurement action is unlawful.

(2) STANDARD OF REVIEW.—The Court shall hold unlawful a covered procurement action taken under sections 1323 or 4713 of this title, in response to a petition that the court finds to be—

(A) arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law;

(B) contrary to constitutional right, power, privilege, or immunity;

(C) in excess of statutory jurisdiction, authority, or limitation, or short of statutory right;

(D) lacking substantial support in the administrative record taken as a whole or in classified information submitted to the court under paragraph (3); or

(E) not in accord with procedures required by law.

(3) EXCLUSIVE JURISDICTION.—The United States Court of Appeals for the District of Columbia Circuit shall have exclusive jurisdiction over claims arising under sections 1323(c)(4) or 4713 of this title against the United States, any United States department or agency, or any component or official of any such department or agency, subject to review by the Supreme Court of the United States under section 1254 of title 28.

(4) ADMINISTRATIVE RECORD AND PROCEDURES.—

(A) IN GENERAL.—The procedures described in this paragraph shall apply to the review of a petition under this section.

(B) ADMINISTRATIVE RECORD.—

(i) FILING OF RECORD.—The United States shall file with the court an administrative record, which shall consist of the information that the appropriate official relied upon in issuing an exclusion or removal order under section 1323(c)(4) or a covered procurement action under section 4713 of this title.

(ii) UNCLASSIFIED, NONPRIVILEGED INFORMATION.—All unclassified information contained in the administrative record that is not otherwise privileged or subject to statutory protections shall be provided to the petitioner with appropriate protections for any privileged or confidential trade secrets and commercial or financial information.

(iii) IN CAMERA AND EX PARTE.—The following information may be included in the administrative record and shall be submitted only to the court ex parte and in camera:

(I) Classified information.

(II) Sensitive security information, as defined by section 1520.5 of title 49, Code of Federal Regulations.

(III) Privileged law enforcement information.

(IV) Information obtained or derived from any activity authorized under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), except that, with respect to such information, subsections (c), (e), (f), (g), and (h) of section 106 (50 U.S.C. 1806), subsections (d), (f), (g), (h), and (i) of section 305 (50 U.S.C. 1825), subsections (c), (e), (f), (g), and (h) of section 405 (50 U.S.C. 1845), and section 706 (50 U.S.C. 1881e) of that Act shall not apply.

(V) Information subject to privilege or protections under any other provision of law.

(iv) UNDER SEAL.—Any information that is part of the administrative record filed ex parte and in camera under clause (iii), or cited by the court in any decision, shall be treated by the court consistent with the provisions of this subparagraph and shall remain under seal and preserved in the records of the court to be made available consistent with the above provisions in the event of further proceedings. In no event shall such information be released to the petitioner or as part of the public record.

(v) RETURN.—After the expiration of the time to seek further review, or the conclusion of further proceedings, the court shall return the administrative record, including any and all copies, to the United States.

(C) EXCLUSIVE REMEDY.—A determination by the court under this subsection shall be the exclusive judicial remedy for any claim described in this section against the United States, any United States department or agency, or any component or official of any such department or agency.

(D) RULE OF CONSTRUCTION.—Nothing in this section shall be construed as limiting, superseding, or preventing the invocation of, any privileges or defenses that are otherwise available at law or in equity to protect against the disclosure of information.

(c) DEFINITION.—In this section, the term "classified information"—

(1) has the meaning given that term in section 1(a) of the Classified Information Procedures Act (18 U.S.C. App.); and

(2) includes—

(A) any information or material that has been determined by the United States Government pursuant to an Executive order, statute, or regulation to require protection against unauthorized disclosure for reasons of national security; and

(B) any restricted data, as defined in section 11 of the Atomic Energy Act of 1954 (42 U.S.C. 2014).

SEC. 1328. TERMINATION.

This subchapter shall terminate on the date that is 5 years after the date of the enactment of the Federal Acquisition Supply Chain Security Act of 2018.

* * * * * * *

DIVISION C—PROCUREMENT

* * * * * * *

CHAPTER 47—MISCELLANEOUS

Sec.

* * * * * * *

SEC. 4712. ENHANCEMENT OF CONTRACTOR PROTECTION FROM REPRISAL FOR DISCLOSURE OF CERTAIN INFORMATION.

* * * * * * *

SEC. 4713. AUTHORITIES RELATING TO MITIGATING SUPPLY CHAIN RISKS IN THE PROCUREMENT OF COVERED ARTICLES.

(a) AUTHORITY.—Subject to subsection (b), the head of an executive agency—

(1) carry out a covered procurement action; and

(2) limit, notwithstanding any other provision of law, in whole or in part, the disclosure of information relating to the basis for carrying out a covered procurement action.

(b) DETERMINATION AND NOTIFICATION.—Except as authorized by subsection (c) to address an urgent national security interest, the head of an executive agency may exercise the authority provided in subsection (a) only after—

(1) obtaining a joint recommendation, in unclassified or classified form, from the chief acquisition officer and the chief information officer of the agency, or officials performing similar functions in the case of executive agencies that do not have such officials, which includes a review of any risk assessment made available by the executive agency identified under section 1323(a)(3) of this title, that there is a significant supply chain risk in a covered procurement;

(2) providing notice of the joint recommendation described in paragraph (1) to any source named in the joint recommendation advising—

(A) that a recommendation is being considered or has been obtained;

(B) to the extent consistent with the national security and law enforcement interests, of information that forms the basis for the recommendation;

(C) that, within 30 days after receipt of the notice, the source may submit information and argument in opposition to the recommendation; and

(D) of the procedures governing the consideration of the submission and the possible exercise of the authority provided in subsection (a);

(3) making a determination in writing, in unclassified or classified form, after considering any information submitted by a source under paragraph (2) and in consultation with the chief information security officer of the agency, that—

(A) use of the authority under subsection (a)(1) is necessary to protect national security by reducing supply chain risk;

(B) less intrusive measures are not reasonably available to reduce such supply chain risk;

(C) a decision to limit disclosure of information under subsection (a)(2) is necessary to protect an urgent national security interest; and

(D) the use of such authorities will apply to a single covered procurement or a class of covered procurements, and otherwise specifies the scope of the determination; and

(4) providing a classified or unclassified notice of the determination made under paragraph (3) to the appropriate congressional committees and leadership that includes—

(A) the joint recommendation described in paragraph (1);

(B) a summary of any risk assessment reviewed in support of the joint recommendation required by paragraph (1); and

(C) a summary of the basis for the determination, including a discussion of less intrusive measures that were considered and why such measures were not reasonably available to reduce supply chain risk.

(c) PROCEDURES TO ADDRESS URGENT NATIONAL SECURITY INTERESTS.—In any case in which the head of an executive agency determines that an urgent national security interest requires the immediate exercise of the authority provided in subsection (a), the head of the agency—

(1) may, to the extent necessary to address such national security interest, and subject to the conditions in paragraph (2)—

(A) temporarily delay the notice required by subsection (b)(2);

(B) make the determination required by subsection (b)(3), regardless of whether the notice required by subsection (b)(2) has been provided or whether the notified source has submitted any information in response to such notice;

(C) temporarily delay the notice required by subsection (b)(4); and

(D) exercise the authority provided in subsection (a) in accordance with such determination within 60 calendar days after the day the determination is made; and

(2) shall take actions necessary to comply with all requirements of subsection (b) as soon as practicable after addressing the urgent national security interest, including—

(A) providing the notice required by subsection (b)(2);

(B) promptly considering any information submitted by the source in response to such notice, and making any appropriate modifications to the determination based on such information;

(C) providing the notice required by subsection (b)(4), including a description of the urgent national security interest, and any modifications to the determination made in accordance with subparagraph (B); and

(D) providing notice to the appropriate congressional committees and leadership within 7 calendar days of the covered procurement actions taken under this section.

(d) DELEGATION.—The head of an executive agency may not delegate the authority provided in subsection (a) or the responsibility identified in subsection (f) to an official below the level one level below the Deputy Secretary or Principal Deputy Director.

(e) LIMITATION ON DISCLOSURE.—If the head of an executive agency has exercised the authority provided in subsection (a)(2) to limit disclosure of information, the agency head or a designee identified by the agency head shall—

(1) provide the executive agency identified by the Council under paragraph (3) of section 1323(a) of this title information identified by the criteria under paragraph (2) of that section, in a manner and to the extent consistent with the requirements of national security and law enforcement interests; and

(2) take steps to maintain the confidentiality of any such notifications.

(f) ANNUAL REVIEW OF DETERMINATIONS.—The head of an executive agency shall conduct an annual review of all determinations made by such head under subsection (b) and promptly amend any covered procurement action as appropriate.

(g) REGULATIONS.—The Federal Acquisition Regulatory Council shall prescribe such regulations as may be necessary to carry out this section.

(h) REPORTS REQUIRED.—Not less frequently than annually, the head of each executive agency that exercised the authority provided in subsection (a) or (c) during the preceding 12-month period shall submit to the appropriate congressional committees and leadership a report summarizing the actions taken by the agency under this section during that 12-month period.

(i) APPLICABILITY.—Notwithstanding section 3101(c)(1)(A) of this title, this section applies to the Department of Defense, the Coast Guard, and the National Aeronautics and Space Administration.

(j) TERMINATION.—The authority provided under subsection (a) shall terminate on the date that is 5 years after the date of the enactment of the Federal Acquisition Supply Chain Security Act of 2018.

(k) DEFINITIONS.—In this section:

(1) APPROPRIATE CONGRESSIONAL COMMITTEES AND LEADERSHIP.—The term "appropriate congressional committees and leadership" means—

(A) the Committee on Homeland Security and Governmental Affairs, the Committee on the Judiciary, the Committee on Appropriations, the Select Committee on Intelligence, and the majority and minority leader of the Senate; and

(B) the Committee on Oversight and Government Reform, the Committee on the Judiciary, the Committee on Appropriations, the Committee on Homeland Security, the Per-

manent Select Committee on Intelligence, and the Speaker and minority leader of the House of Representatives.

(2) COVERED ARTICLE.—The term covered article means—

(A) information technology, as defined in section 11101 of title 40, including cloud computing services of all types;

(B) telecommunications equipment or telecommunications service, as those terms are defined in section 3 of the Communications Act of 1934 (47 U.S.C. 153);

(C) the processing of information of a Federal or non-Federal information system, subject to the requirements of the Controlled Unclassified Information program; or

(D) hardware, systems, devices, software, or services that include embedded or incidental information technology.

(3) COVERED PROCUREMENT.—The term "covered procurement" means—

(A) a source selection for a covered article involving either a performance specification, as provided in subsection (a)(3)(B) of section 3306 of this title, or an evaluation factor, as provided in subsection (b)(1)(A) of such section, relating to a supply chain risk, or where supply chain risk considerations are included in the agency's determination of whether a source is a responsible source as defined in section 113 of this title;

(B) the consideration of proposals for and issuance of a task or delivery order for a covered article, as provided in section 4106(d)(3) of this title, where the task or delivery order contract includes a contract clause establishing a requirement relating to a supply chain risk;

(C) any contract action involving a contract for a covered article where the contract includes a clause establishing requirements relating to a supply chain risk; or

(D) any other procurement in a category of procurements determined appropriate by the Federal Acquisition Regulatory Council, with the advice of the Federal Acquisition Security Council.

(4) COVERED PROCUREMENT ACTION.—The term "covered procurement action" means any of the following actions, if the action takes place in the course of conducting a covered procurement:

(A) The exclusion of a source that fails to meet qualification requirements established under section 3311 of this title for the purpose of reducing supply chain risk in the acquisition or use of covered articles.

(B) The exclusion of a source that fails to achieve an acceptable rating with regard to an evaluation factor providing for the consideration of supply chain risk in the evaluation of proposals for the award of a contract or the issuance of a task or delivery order.

(C) The determination that a source is not a responsible source as defined in section 113 of this title based on consideration of supply chain risk.

(D) The decision to withhold consent for a contractor to subcontract with a particular source or to direct a contractor to exclude a particular source from consideration for a subcontract under the contract.

(5) INFORMATION AND COMMUNICATIONS TECHNOLOGY.—The term "information and communications technology" means—

(A) information technology, as defined in section 11101 of title 40;

(B) information systems, as defined in section 3502 of title 44; and

(C) telecommunications equipment and telecommunications services, as those terms are defined in section 3 of the Communications Act of 1934 (47 U.S.C. 153).

(6) SUPPLY CHAIN RISK.—The term "supply chain risk" means the risk that any person may sabotage, maliciously introduce unwanted function, extract data, or otherwise manipulate the design, integrity, manufacturing, production, distribution, installation, operation, maintenance, disposition, or retirement of covered articles so as to surveil, deny, disrupt, or otherwise manipulate the function, use, or operation of the covered articles or information stored or transmitted on the covered articles.

* * * * * * *

TITLE 44—PUBLIC PRINTING AND DOCUMENTS

* * * * * * *

CHAPTER 35—COORDINATION OF FEDERAL INFORMATION POLICY

* * * * * * *

Subchapter II—Information Security

* * * * * * *

SEC. 3553. AUTHORITIES AND FUNCTIONS OF THE DIRECTOR AND SECRETARY.

(a) * * *

(1) * * *

* * * * * * *

(5) overseeing agency compliance with the requirements of this subchapter *and section 1326 of title 41*, including through any authorized action under section 11303 of title 40, to enforce accountability for compliance with such requirements; and

* * * * * * *

SEC. 3554. FEDERAL AGENCY RESPONSIBILITIES.

(a) * * *

(1) * * *

(A) * * *

(B) complying with the requirements of this subchapter, *subchapter III of chapter 13 of title 41*, and related policies, procedures, standards, and guidelines, including—

(i) * * *

(ii) * * *

(iii) * * *

(iv) information security standards and guidelines for national security systems issued in accordance with law and as directed by the President[; and]*;*

(v) * * *

(vi) responsibilities relating to assessing and avoiding, mitigating, transferring, or accepting supply chain risks under section 1326 of title 41, and complying with exclusion and removal orders issued under section 1323 of such title; and

* * * * * * *

○