DEPA

GENERAL SERVICES ADMINISTRATION

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

48 CFR Parts 1, 2, 4, 7, 10, 11, 12, 39, and 52

[FAR Case 2021-017; Docket No. FAR-2021-0017; Sequence No. 1]

RIN 9000-AO34

Federal Acquisition Regulation: Cyber Threat and Incident Reporting and Information Sharing

AGENCY: Department of Defense (DoD), General Services Administration (GSA), and National Aeronautics and Space Administration (NASA).

ACTION: Proposed rule.

SUMMARY: DoD, GSA, and NASA are proposing to amend the Federal Acquisition Regulation (FAR) to partially implement an Executive order on cyber threats and incident reporting and information sharing for Federal contractors and to implement related cybersecurity policies.

DATES: Interested parties should submit written comments to the Regulatory Secretariat Division at the address shown below on or before **[INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]** to be considered in the formation of the final rule.

ADDRESSES: Submit comments in response to FAR Case 2021-017 to the Federal eRulemaking portal at *https://www.regulations.gov* by searching for "FAR Case

2021-017". Select the link "Comment Now" that corresponds with "FAR Case 2021-017". Follow the instructions provided on the "Comment Now" screen. Please include your name, company name (if any), and "FAR Case 2021-017" on your attached document. If your comment cannot be submitted using *https://www.regulations.gov*, call or email the points of contact in the FOR FURTHER INFORMATION CONTACT section of this document for alternate instructions.

Instructions: Please submit comments only and cite "FAR Case 2021-017" in all correspondence related to this case. Comments received generally will be posted without change to *https://www.regulations.gov*, including any personal and/or business confidential information provided. Public comments may be submitted as an individual, as an organization, or anonymously (see frequently asked questions at *https://www.regulations.gov/faq*). To confirm receipt of your comment(s), please check *https://www.regulations.gov*, approximately two to three days after submission to verify posting.

FOR FURTHER INFORMATION CONTACT: For clarification of content, contact Ms. Marissa Ryba, Procurement Analyst, at 314-586-1280 or by email at *Marissa.Ryba@gsa.gov*. For information pertaining to status, publication schedules, or alternate instructions for submitting comments if *https://www.regulations.gov* cannot be used, contact the

Regulatory Secretariat Division at 202-501-4755 or *GSARegSec@gsa.gov*. Please cite FAR Case 2021-017.

SUPPLEMENTARY INFORMATION:

I. Background

DoD, GSA, and NASA are proposing to revise the FAR to increase the sharing of information about cyber threats and incident information between the Government and information technology and operational technology service providers, pursuant to Executive Order (E.O.) 14028, Improving the Nation's Cybersecurity. The E.O. was signed by the President on May 12, 2021, and published in the *Federal Register* at 86 FR 26633 on May 17, 2021.

The E.O. is focused on improving the nation's cybersecurity, in part through increased protection of Government networks. As directed in sections 2(d) and 2(g)(ii) of the E.O., this proposed rule implements Office of Management and Budget (OMB) recommendations from section 2(b) of the E.O., and Cybersecurity and Infrastructure Security Agency (CISA) recommendations from section 2(g)(i) of the E.O. This proposed rule considers recommendations issued by the Department of Homeland Security (DHS) pursuant to section 8(b). CISA is an agency within DHS. Additionally, this proposed rule supports implementation of the National Cyber Strategy by strengthening and standardizing contract requirements for cybersecurity and by providing mechanisms to help ensure that entities or

individuals that knowingly put U.S. information or systems at risk, by violating these cybersecurity requirements, are held accountable. Finally, this proposed rule implements OMB Memorandum M-21-07, Completing the Transition to Internet Protocol Version 6 (IPv6), dated November 19, 2020.

Recent cybersecurity incidents such as those involving SolarWinds, Microsoft Exchange, and the Colonial Pipeline incident are a sobering reminder that U.S. public and private sector entities increasingly face sophisticated malicious cyber activity from both nation-state actors and cyber criminals. These incidents share commonalities, including insufficient cybersecurity defenses that leave public and private sector entities more vulnerable to incidents. The E.O. makes a significant contribution toward modernizing cybersecurity defenses by protecting Federal networks, improving information sharing between the U.S. Government and the private sector on cyber issues, and strengthening the United States' ability to respond to incidents when they occur. This proposed rule underscores that the compliance with information-sharing and incident-reporting requirements are material to eligibility and payment under Government contracts.

II. Discussion and Analysis

The following summarizes the proposed changes to the FAR:

FAR 2.101 currently defines *information and communication technology* as information technology and other equipment, systems, technologies, or processes, for which the principal function is the creation, manipulation, storage, display, receipt, or transmission of electronic data and information, as well as any associated content. Examples include, but are not limited to, the following: Computers and peripheral equipment; information kiosks and transaction machines; telecommunications equipment; customer premises equipment; multifunction office machines; software; applications; websites; videos; and electronic documents. This definition was implemented in FAR case 2017-011 (August 11, 2021, 86 FR 44229, effective September 10, 2021). It has examples primarily aimed at section 508 of the Rehabilitation Act of 1973. This FAR case proposes to change the term defined in FAR 2.101 to *information and communications technology (ICT)* and to provide additional examples not primarily aimed at section 508: *telecommunications services, electronic media, internet of things (IoT) devices, and operational technology*. This definition is also proposed to be updated to revise the term *software* to *computer software* to align with the previously defined term of *computer software* in 2.101.

The definition of *information system* currently appearing at 4.1901 is proposed to be moved to 2.101 with a slight revision to the statutory citation.

New definitions are proposed to be added for *IoT devices* (derived from section 2 of Pub. L. 116-207), *operational technology* (derived from NIST SP 800-160 vol. 2), *telecommunications equipment* (derived from DFARS subpart 239.74), and *telecommunications services* (derived from DFARS subpart 239.74). Additionally, these proposed definitions, except for IoT devices will be incorporated into the new clause. FAR Case 2021-019, Standardizing Cybersecurity Requirements for Unclassified Federal Information Systems, which also implements sections of E.O. 14028, is proposing to add some of the same definitions.

FAR 7.105, Contents of written acquisition plans, is proposed to be updated to show the IPv6 coverage move to 39.106.

FAR 11.002, Policy at subparagraph (g) is proposed to be revised to point to the IPv6 coverage move.

FAR 12.202, Market research and description of agency need, is proposed to be updated to show the IPv6 coverage move.

FAR 39.001, Applicability, is proposed to be revised to explain that the exceptions and exemptions at subpart 39.2 only apply to subpart 39.2.

FAR 39.002, Definitions, is proposed to be updated to add the definition of *Supplier's declaration of conformity* as derived from NIST SP 500-281B.

FAR 39.101, Policy, is proposed to be updated to show the IPv6 coverage move.

FAR 39.106, Contract clause, is proposed to be replaced with a new section, Internet Protocol version 6 (IPv6). Sections are added at 39.106-1, Policy and 39.106-2, Waiver of IPv6 requirements. This is a revision of coverage moved from FAR 11.002(g). (IPv6 is also covered in the new clause.)

A new section is proposed to be added at 39.107, Response to incident reports and requests for information or access.

The prescription for the contract clause at 52.239-1, Privacy or Security Safeguards, is proposed to be moved from 39.106 to 39.108 and designated paragraph (a). The prescription for the new contract clause at 52.239-ZZ, Incident and Threat Reporting and Incident Response Requirements for Products or Services Containing Information and Communications Technology, is proposed to be added at paragraph (b), and the prescription for the new solicitation provision at 52.239-AA, Security Incident Reporting Representation, is proposed to be added at paragraph (c).

The provision at 52.212-3, Offeror Representations and Certifications—Commercial Products and Commercial Services, is proposed to be revised to add definitions for information and communications technology, security

incident and security incident reports. This provision is also proposed to be updated to require offerors to represent that they have submitted all security incident reports in a current, accurate and complete manner; and represent that they have required each lower-tier subcontractor under certain contracts to include the requirements of paragraph (f) of FAR clause 52.239-ZZ in their subcontract.

The clause at 52.212-5, Contract Terms and Conditions Required to Implement Statutes or Executive Orders--Commercial Products and Commercial Services, is proposed to be revised to add the commercial product and service usage of the new clause 52.239-ZZ, including flow down to subcontracts.

The clause at 52.213-4, Terms and Conditions—Simplified Acquisitions (Other Than Commercial Products and Commercial Services), is proposed to be revised to add the commercial product and service usage of the new clause 52.239-ZZ, including flow down to subcontracts.

The prescription reference for the clause 52.239-1, Privacy or Security Safeguards, is proposed to be updated.

A new provision at FAR 52.239-AA, Security Incident Reporting Representation, is proposed to be added to require offerors to represent that they have submitted all security incident reports in a current, accurate and complete manner; and represent whether they have required

each lower-tier subcontractor to include the requirements of paragraph (f) of FAR clause 52.239-ZZ in their subcontract.

A new clause at FAR 52.239-ZZ, Incident and Threat Reporting and Incident Response Requirements for Products or Services Containing Information and Communications Technology, is proposed to be added as required by section 2(a) of E.O. 14028. It establishes new definitions and coverage for: requests for security incident reporting; supporting incident response; cyber threat indicators and defensive measures reporting; and IPv6.

The clause at 52.244-6, Subcontracts for Commercial Products and Commercial Services, is proposed to be revised to add the subcontract flowdown prescription for commercial product and service usage of the new clause 52.239-ZZ.

a. Software Bills of Materials

This rule proposes a new requirement for contractors to develop and maintain a software bill of materials (SBOM) for any software used in the performance of the contract regardless of whether there is any security incident. SBOMs are described at section 10(j) of E.O. 14028. Further information is available at the website listed at paragraph (c)(3)(i) of 52.239-ZZ. These SBOMs can be critical in incident response, as they allow for prompt identification of any sources of a known vulnerability. Recognizing the potential impact of this requirement, DoD, GSA, and NASA

welcome input on the following questions regarding anticipated impact of including a requirement to develop SBOMs:

- How should SBOMs be collected from contractors? What specific protections are necessary for the information contained within an SBOM?
- How should the Government think about the appropriate scope of the requirement on contractors to provide SBOMs to ensure appropriate security?
- What challenges will contractors face in the development of SBOMs? What challenges are unique to software resellers? What challenges exist regarding legacy software?
- What are the appropriate means of evaluating when an SBOM must be updated based on changes in a new build or major release?
- What is the appropriate balance between the Government and the contractor, when monitoring SBOMs for embedded software vulnerabilities as they are discovered?

b. CISA Engagement Services

The rule proposes requirements that will include access by and cooperation with CISA engagement services related to threat hunting and incident response. The requirements in this proposed rule provide mechanisms whereby such access and cooperation can be initiated by

CISA. The primary purpose of this interaction is providing visibility into systems to observe adversary activity, which helps CISA drive risk reduction. CISA engagement reports may contain recommendations regarding compromised systems.

It is expected that any action taken in response to such recommendations would only be taken after consultation between the contractor and the contracting agency, including both the requiring activity and the contracting officer.

c. Access to Contractor Information and Information Systems

Through operation of paragraph (c)(6) of the clause at FAR 52.239-ZZ, this proposed rule provides CISA, the Federal Bureau of Investigation (FBI) in the Department of Justice, and the contracting agency full access to applicable contractor information and information systems, and to contractor personnel, in response to a security incident reported by the contractor or a security incident identified by the Government, as required by the E.O.

DoD, GSA, and NASA welcome input on the following questions:

- Do you have any specific concerns with providing CISA, the FBI, or the contacting agency full access (see definition at 52.239-ZZ(a)) information, equipment, and to contractor personnel? Please

provide specific details regarding any concerns associated with providing such access.

- For any specific concerns identified, are there any specific safeguards, including safeguards that would address the scope of full access or how full access would be provided, that would address your concerns while still providing the Government with appropriate access to conduct necessary forensic analysis regarding security incidents?
- Subparagraph (g)(i)(C) of section 2 of E.O. 14028 recognizes the need to identify appropriate and effective protections for privacy and civil liberties. Are there any specific safeguards that should be considered to ensure that these protections are effectively accomplished?

d. Compliance When Operating in a Foreign Country

The proposed rule requires contractors and subcontractors to report security incidents and take additional actions to support incident response. DoD, GSA, and NASA recognize that contractors operating in certain foreign countries may be subject to laws and regulations from those countries regarding what information and access can be provided to the U.S. Government.

For example, a vendor based in a foreign country may be part of the defense industrial base for that foreign country while also doing work for the U.S. Government as a

subcontractor. Another example could be where a subcontractor produces an ICT product in a foreign country that prevents the supplier from sending information or data located in that foreign country to the U.S. Government.

DoD, GSA, and NASA are considering, for purposes of the final rule, options to address this issue.

DoD, GSA, and NASA welcome input on the following questions:

- Are there any specific situations you anticipate where your organization would be prevented from complying with the incident reporting or incident response requirements of FAR 52.239-ZZ due to country laws and regulations imposed by a foreign government? If so, provide specific examples that identify which requirements would be impacted and the reason that compliance would be prevented by the laws of a foreign government or operating environment within a foreign country.
- Do you anticipate situations where compliance with requirements in FAR 52.239-ZZ or alternative compliance methods (if added) would be prevented due to country laws and regulations imposed by a foreign government. If so, provide specific examples of when you expect such situations to occur, citing the authoritative source from the foreign government.

e. Security Incident Reporting Harmonization

The Government needs to be aware of compromises of its data and the systems operated on behalf of the Government as soon as possible. Because compromises of the ICT described in this proposed rule can sometimes undermine Government network resilience and agency missions, the proposed rule requires contractors to "immediately and thoroughly investigate all indicators that a security incident may have occurred and submit information using the CISA incident reporting portal…within eight hours of discovery…[and to] update the submission every 72 hours thereafter until the Contractor, the agency, and/or any investigating agencies have completed all eradication or remediation activities."

Timely incident reporting promotes the security and resilience of Government networks by facilitating rapid data analysis to promptly identify activity and actions of malicious actors, threats, and indicators of compromise. Recognizing that initial reports may not contain complete information, even incomplete early reports provide the Government an important opportunity to limit the extent of damage to its systems and data. Subsequent reporting throughout the lifecycle of the incident ensures the Government is able to take the full measure of appropriate actions.

Given the ubiquity of ICT in products and services, contractors may offer products and services to the

Government that are subject to additional incident reporting requirements imposed by other contracts or regulatory regimes. When the same underlying systems are subject to inconsistent or contradictory incident reporting requirements--or where such requirements are duplicative but enforced differently by different counterparties or regulators--companies may focus more on compliance than on security, which can result in passing higher costs on to customers, including the Government.

DoD, GSA, and NASA recognize there are various reporting timeframes for cyber incidents across the Government and industry, including the Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012, which requires reporting of the compromise of DoD controlled unclassified information (CUI) (only cyber incidents) within 72 hours of discovery; the Homeland Security Acquisition Regulation (HSAR), which requires contractors to report any cybersecurity incident that could affect CUI within eight hours (or one hour if it involves personally identifiable information); the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), currently the subject of a separate rulemaking process (see 6 U.S.C. 681b(b)), which states that a "covered entity that experiences a covered cyber incident shall report the covered cyber incident to the Agency not later than 72 hours after the covered entity reasonably believes that the

covered cyber incident has occurred"; and the National Industrial Security Program Operating Manual (NISPOM), which requires "promptly" reporting cyber incidents involving classified information (no specified time). The products and systems that contractors offer to the Federal Government may be subject to these and other incident reporting requirements.

DOD, GSA, and NASA welcome public comment on incident reporting harmonization, including answers to the following questions:

- Timeline for reporting: Are there specific situations you anticipate where your organization will be required to report on different timelines in order to comply with the incident reporting requirements outlined in 52.239-ZZ, other Federal contract requirements, or other regulations promulgated under Federal law? How would your organization handle disparate cyber incident reporting timelines in other Federal Government contracting requirements or from other regulatory agencies?

- Potential effect on incident response: Incident response and associated reporting are often iterative processes, with system owners updating reports as a situation evolves and more data becomes available. What implications are there for your organization, including with respect to incident response, to meet disparate timelines for incident reporting?

- Cost of providing ICT products and services: How much, if at all, would you estimate that the initial reporting requirement described in this proposed rule could increase the price of the products or services your organization provides to the Federal Government?
- Scope of the contract clause: The proposed rule would require the new incident reporting clause to be included in all contracts involving ICT that are subject to the FAR, including those for commercially available off-the-shelf (COTS) items. This is broader in scope than, for instance, the DFARS clause. How would differences in scope between reporting requirements affect your organization's implementation of this clause?
- Definition of incident: The definition of "security incident" in the proposed rule incorporates the substantive provisions of the definition in 44 U.S.C. 3552, which has minor differences from with the definition of "incident" in Section 2209 of the Homeland Security Act of 2002 (as amended) and from the modified definition of "covered incident" used in CIRCIA, which is currently the subject of a separate rulemaking process, see 6 U.S.C. 681b(b). What, if any, additional implementation issues would your entity face complying with different definitions of an incident? How would your entity make the distinction between "imminent jeopardy" and "actual jeopardy," and what effect could that have on the number of reported incidents

that did not end up actually affecting confidentiality, integrity, and availability of information or an information system?

III. Applicability to Contracts at or Below the Simplified Acquisition Threshold (SAT) and for Commercial Products, Including Commercially Available Off-the-Shelf (COTS) Items, or for Commercial Services

This rule proposes to add a new clause at FAR 52.239-ZZ, Incident and Threat Reporting and Incident Response Requirements for Products or Services Containing Information and Communications Technology. The clause is prescribed at FAR 39.108(b) for use in all contracts and solicitations. Contracting officers will be required to use the clause in solicitations and contracts below the simplified acquisition threshold, and for commercial products, including COTS items, and for commercial services.

IV. Expected Impact of the Rule

The purpose of this proposed rule is to partially implement E.O. 14028, Improving the Nation’s Cybersecurity. Section 1 of the E.O. states: “The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people’s security and privacy. The Federal Government must improve its efforts

to identify, deter, protect against, detect, and respond to these actions and actors."

As businesses store more of their and their Federal Government customers' data online, they are becoming increasingly vulnerable to cyber thieves. Dealing with online criminals increases cybersecurity costs, which ultimately is passed down to the Federal Government in the form of higher prices. Studies have shown several ways that a company's failure to protect valuable data can harm their customers. Among these are lost revenue, increased costs, stolen intellectual property, and operational disruption.

DoD, GSA, and NASA have performed a regulatory impact analysis (RIA) on this proposed rule. The total estimated public costs associated with this proposed FAR rule in millions calculated over a ten-year period (calculated at a 3-percent and 7-percent discount rate) are as follows:

SUMMARY	Public	Government	Total
Present Value (3 percent)	$8,644 Million	$225 Million	$ 8,869 Million
Annualized Costs (3 percent)	$1,013 Million	$26 Million	$1,039 Million
Present Value (7 percent)	$7,194 Million	$185 Million	$7,379 Million
Annualized Costs (7 percent)	$1,024 Million	$26 Million	$1,050 Million

The following is a summary from the RIA of the specific compliance requirements and the estimated costs of compliance. The RIA includes a detailed discussion and explanation about the assumptions and methodology used to estimate the cost of this regulatory action, including the specific impact and costs for small businesses. It is available at *https://www.regulations.gov* (search for "FAR Case 2021-017" click "Open Docket," and view "Supporting Documents").

This proposed rule will impact all contractors awarded contracts where ICT is used or provided in the performance of the contract. The Government does not have a way to track awards that may include ICT in support of the product or service being offered to the Government, so DoD, GSA, and NASA assume that 75 percent of all entities are awarded contracts that include some ICT. Of the 75 percent of entities awarded contracts with some ICT, it is assumed that 4 percent of those entities may have a reportable cyber incident.

The portions of this proposed rule that are related to cyber incident reporting, in some cases, are estimated to apply to a smaller percentage of the 4 percent of unique entities (i.e., 10 percent, 20 percent, 40 percent, or 50 percent of the 4 percent) that have awards containing some ICT, because some compliance activities are only necessary

if required by the Government. For example, it is assumed that 10 percent of the 4 percent will be required to provide access for additional information for forensic analysis, 20 percent of the 4 percent will be required to provide incident damage assessment information, 40 percent of the 4 percent will be required to submit malicious code samples, and 50 percent of the 4 percent will be required to develop, store, and maintain customization files and provide to the Government. The Government does not have precise quantifiable data that will represent Government requests related to the various compliance activities, but DoD, GSA, and NASA have included these factors as assumptions based on subject matter expert input to reflect that the requirements will be variable depending on the Government's needs.

The primary cost impact of this proposed rule is that contractors awarded contracts that include ICT will be required to conduct the activities below in accordance with FAR clause 52.239-ZZ, as required.

Security Incident Reporting

Contractors awarded contracts that include ICT and experience a reportable security incident shall support security incident reporting by:

- Providing information regarding reportable incidents to the CISA incident reporting portal at *https://www.cisa.gov/report* and to affected

agencies, to include providing any updates until eradication or remediation activities are completed;

- Conducting data preservation and protection and providing that information to the Government, if requested;
- Developing, storing, and maintaining customization files, and providing to the Government, if requested;
- Providing to the Government and any 3rd party authorized assessor all incident and damage assessment information, if the Government elects to conduct an incident or damage assessment;
- Submitting malicious code samples or artifacts to CISA using the form at *https://www.malware.us-cert.gov* within 8 hours of discovery and isolation of the malicious software. Note that the response time for reporting security incidents is 8 hours; and
- Providing access to additional information or equipment necessary for forensic analysis, upon request by the Government, and time to cooperate with the Government on ensuring effective incident response, corrections, or fixes and time to confirm validity of request from CISA and/or the FBI and notifying the contracting officer.

Security Incident Preparation

In addition, regardless of whether a reportable security incident occurs, contractors for which the clause is prescribed will be required to conduct the preparation and maintenance activities described below.

Contractors awarded contracts that include ICT shall support cyber incident reporting, should an incident occur in the future, by:

- Providing and maintaining a software bill of materials (SBOM);
- Subscribing to the automated indicator sharing (AIS) capability or successor technology during the performance of the contract; and
- Sharing cyber threat indicators and recommended defensive measures in an automated fashion using AIS during the performance of the contract.

IPv6 Implementation

In addition, contractors for which the clause is prescribed will also be required to complete the following IPv6 implementation activities, as required.

The United States Government is transitioning to deliver its information services, operate its networks, and access the services of others using only IPv6 (see OMB Memorandum M-21-07, Completing the Transition to Internet Protocol Version 6 (IPv6), dated November 19, 2020). Contractors awarded contracts that include ICT products and

services that use internet protocols will implement IPv6 by:

- Providing IPv6 capabilities required (see USGv6 Profile NIST SP 500-267B) support the Government's transition to IPv6 (OMB Memorandum M-21-07);
- Documenting the IPv6 capabilities provided by submitting a corresponding supplier's declaration of conformity, in accordance with the USGv6 Test Program (see NIST SP 500-281A); and
- Developing and providing an IPv6 Implementation Plan to the Government that details how the contractor plans to incorporate applicable required capabilities recommended in the current version of NIST SP 500-267B into products and services provided to the Government, for contracts for which the agency CIO has approved a waiver of the IPv6 requirements above.

Benefits of This Proposed Rule

The theft of intellectual property and sensitive information from all U.S. industrial sectors due to malicious cyber activity threatens economic security and national security. The Council of Economic Advisors estimates that malicious cyber activity costs the U.S. economy between $57 billion and $109 billion in 2016. Over a ten-year period, that burden would equate to an estimated $570 billion to $1.09 trillion dollars in costs. The

purpose of this proposed rule is to protect the nation's economic and national security which can result in long-term economic and national security impacts.

Furthermore, the purpose of this proposed rule is to partially implement Executive Order (E.O. 14028, Improving the Nation's Cybersecurity. E.O. 14028 states:

> "The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace. In the end, the trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is, and to the consequences we will incur if that trust is misplaced.
>
> Incremental improvements will not give us the security we need; instead, the Federal Government needs to make bold changes and significant investments in order to defend the vital institutions that underpin the American way of life. The Federal Government must bring to bear the full scope of its authorities and resources to protect and secure its computer systems, whether they are cloud-based, on-premises, or hybrid. The scope of protection and security must include systems that process data (information technology (IT)) and those that run the vital machinery that ensures our safety (operational technology (OT)).
>
> It is the policy of my Administration that the prevention, detection, assessment, and remediation of cyber incidents is a top priority and essential to national and economic security. The Federal Government must lead by example. All Federal Information Systems should meet or exceed the standards and requirements for cybersecurity set forth in and issued pursuant to this order."

IPv6 is the next-generation Internet protocol, designed to replace version 4 (IPv4) that has been in use since 1983. The global demand for IP addresses has grown

exponentially with the ever-increasing number of users, devices, and virtual entities connecting to the Internet, resulting in the exhaustion of readily available IPv4 addresses. A full transition to IPv6 is the only viable option to ensure future growth and innovation in Internet technology and services.

V. Executive Orders 12866 and 13563

Executive Orders (E.O.s) 12866 and 13563 direct agencies to assess all costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributive impacts, and equity). E.O. 13563 emphasizes the importance of quantifying both costs and benefits, of reducing costs, of harmonizing rules, and of promoting flexibility. This is a significant regulatory action under section 3(f)(1) of E.O. 12866, Regulatory Planning and Review, dated September 30, 1993, as amended by E.O. 14094, Modernizing Regulatory Review, and, therefore, was subject to review under Section 6(b) of E.O. 12866.

VI. Regulatory Flexibility Act

This proposed rule, when finalized, may have a significant economic impact on a substantial number of small entities within the meaning of the Regulatory Flexibility Act, 5 U.S.C. 601-612. An Initial Regulatory

Flexibility Analysis (IRFA) has been performed and is summarized as follows:

DoD, GSA, and NASA are proposing to revise the FAR to increase the sharing of information about cyber threats and incident information between the Government and information technology and operational technology service providers, pursuant to Executive Order 14028, Improving the Nation's Cybersecurity (the E.O.). The E.O. was signed by the President on May 12, 2021, and published in the Federal Register at 86 FR 26633 on May 17, 2021.

The E.O. is focused on improving the nation's cybersecurity, in part through increased protection of Federal Government networks. This proposed rule would implement sections 2(d) (implementing OMB recommendations from section 2(b)) and 2(g)(ii) (implementing CISA recommendations from section 2(g)(i)) of the E.O., including consideration of the recommendations issued by the DHS pursuant to section 8(b). Additionally, this proposed rule would implement related cybersecurity policy in OMB Memorandum M-21-07, Completing the Transition to Internet Protocol Version 6 (IPv6), dated November 19, 2020.

Recent cybersecurity incidents such as those involving SolarWinds, Microsoft Exchange, and the Colonial Pipeline incident are a sobering reminder that U.S. public and private sector entities increasingly face sophisticated malicious cyber activity from both nation-state actors and cyber criminals. These incidents share commonalities, including insufficient cybersecurity defenses that leave public and private sector entities more vulnerable to incidents. The E.O. makes a significant contribution toward modernizing cybersecurity defenses by protecting Federal networks, improving information-sharing between the U.S. Government and the private sector on cyber issues, and strengthening the United States' ability to respond to incidents when they occur.

The objective is to implement sections 2(d) and 2(g)(ii), of Executive Order 14028. Promulgation of the FAR authorized by 40 U.S.C. 121(c); 10 U.S.C. chapter 4 and 10 U.S.C. chapter 137 legacy provisions (see 10 U.S.C. 3016); and 51 U.S.C. 20113.

The proposed rule may affect a portion of entities that contract with the Federal Government. Based on data obtained from the Federal Procurement Data System for fiscal years 2019 through 2021, an average of 94,035 entities, of which 61,797 are small entities, were awarded Federal contracts. It is assumed that 75 percent of the 94,035 entities awarded contracts are awarded contracts with some ICT, or 70,526 entities, of which 46,348 are small business entities. Portions of this proposed rule would apply to the 70,526 entities, including the 46,348 small business entities.

In addition, DoD, GSA, and NASA estimate that portions of the proposed rule will apply to different percentages of the 70,526 entities depending on how often the Government requests the data and information associated with each requirement.

The proposed rule would institute compliance requirements for contractors to implement requirements to support incident response and to submit information on all reportable incidents involving a product or service provided to the Government that includes ICT, or the information system used in developing or providing the product or service.

The Government has no way to know how often a particular requirement will impact the public, except for estimates of 4 percent for cyber incident reporting and 40 percent for malware submission based on historical data, but the Government otherwise assumes the impact for other activities will occur for 10 percent, 20 percent, or 50 percent of the entities that have contract awards containing ICT for which there is a reportable cyber incident. The portions of this proposed rule that are related to cyber incident reporting, in some cases, are estimated will apply to a smaller percentage of the 4 percent of unique entities (i.e., 10 percent, 20 percent, 40 percent, or 50 percent of the 4 percent) that have awards containing some ICT, because some compliance activities are only necessary if required by the Government. For example, it is assumed that 10 percent of the 4percent will be required to provide access for additional information for forensic analysis, 20 percent of the 4 percent will be required to provide incident damage assessment information, 40 percent of the 4 percent will be required to submit malicious code samples, and 50 percent of the 4 percent will be required to develop, store, and maintain customization files, and provide to the Government. The Government does not have precise quantifiable data that will represent Government requests related to the various compliance activities but DoD, GSA, and NASA have included these factors as assumptions to reflect that the requirements will be variable depending on the Government's needs.

This proposed rule will establish safeguards that will increase the sharing of information about cyber threats and incident information between the Government and information technology and operational technology service providers.

The proposed rule includes reporting or recordkeeping requirements. The following are compliance requirements of the proposed rule:

(a) Regulatory familiarization.

(b) 52.239-ZZ, paragraph (b), for contractors to support security incident reporting including: providing information regarding reportable incidents to CISA at *https://www.cisa.gov/report*, and to affected agencies, and any updates until eradication or remediation activities are completed.

(c) 52.239-ZZ, paragraph (c)(1), for contractors to support incident response by conducting data preservation and protection and providing to the Government, if requested.

(d) 52.239-ZZ, paragraph (c)(2), for contractors to support incident response by developing, storing,

and maintaining customization files, and providing to the Government, if requested.

(e) 52.239-ZZ, paragraph (c)(3), for contractors to support incident response by developing and maintaining a software bill of materials (SBOM) and providing or providing access to the SBOM (and its updates) to the Government.

(f) 52.239-ZZ, paragraph (c)(4), for contractors to support incident response by providing to the Government and any 3rd party authorized assessor all incident and damage assessment information identified in clause paragraphs (c)(1)-(3), if the Government elects to conduct an incident or damage assessment.

(g) 52.239-ZZ, paragraph (c)(5), for contractors to support incident response by, if applicable, submitting malicious code samples or artifacts to CISA using the form at *https://www.malware.us-cert.gov* within 8 hours of discovery and isolation of the malicious software.

(h) 52.239-ZZ, paragraph (c)(6), for contractors to support incident response by providing access (see (c)(6)(i)) to additional information or equipment necessary for forensic analysis, upon request by the Government, and time to cooperate with the Government on ensuring effective incident response, corrections, or fixes, and time (see (c)(6)(ii)) to confirm validity of request from CISA by contacting the CISA Hotline and notifying the contracting officer.

(i) 52.239-ZZ, paragraph (d)(1), for contractors to support incident response by subscribing to the Automated Indicator Sharing (AIS) capability or successor technology during the performance of the contract.

(j) 52.239-ZZ, paragraph (d)(2), for contractors to support incident response by sharing cyber threat indicators and recommended defensive measures in an automated fashion using AIS during the performance of the contract.

(k) 52.239-ZZ, paragraph (e) for contractors to support incident response by implementing delta capabilities required for moving to IPv6 for ICT products and services using internet protocol (capabilities in NIST SP 500-267B).

(l) 52.239-ZZ, paragraph (e) for contractors to provide a corresponding supplier’s declaration of conformity in accordance with the USGv6 Test Program (see NIST SP 500-281A).

(m) 52.239-ZZ, paragraph (e) for contractors, for which the agency CIO has approved a waiver of IPv6 requirements, to develop and provide an IPv6 Implementation Plan to the Government that details how the contractor plans to incorporate applicable

mandatory capabilities recommended in the current version of NIST SP 500-267B into products and services provided to the Government.

(n) 52.239-AA, paragraph (b) for offerors to represent that they have submitted all security incident reports in a current, accurate and complete manner; and represent that they have required each lower-tier subcontractor to include the requirements of paragraph (f) of FAR clause 52.239-ZZ in their subcontract.

The proposed rule would not duplicate, overlap, or conflict with any other Federal rules.

There are no available alternatives to the proposed rule identified to accomplish the desired objective of the E.O. 14028.

The Regulatory Secretariat Division has submitted a copy of the IRFA to the Chief Counsel for Advocacy of the Small Business Administration. A copy of the IRFA may be obtained from the Regulatory Secretariat Division. DoD, GSA, and NASA invite comments from small business concerns and other interested parties on the expected impact of this proposed rule on small entities.

DoD, GSA, and NASA will also consider comments from small entities concerning the existing regulations in subparts affected by the rule in accordance with 5 U.S.C. 610. Interested parties must submit such comments separately and should cite 5 U.S.C. 610 (FAR Case 2021-017), in correspondence.

VII. Paperwork Reduction Act

The Paperwork Reduction Act (44 U.S.C. 3501-3521) applies because the proposed rule contains information collection requirements. Accordingly, the Regulatory Secretariat Division has submitted a request for approval of a new information collection requirement concerning

incident and threat reporting and incident response requirements to the Office of Management and Budget. The annual reporting burden is estimated as follows:

A. Public burden for this collection of information:

(1) Submitting information regarding reportable incidents to be included in the CISA incident reporting portal at *https://www.cisa.gov/report*.

DoD, GSA, and NASA estimate that providing this information will take 4 hours applied to 2,821 entities, of which 1,854 are small business entities. The number of entities are assumed based on an assumption that 75 percent of all entities awarded contracts (94,035) are awarded contracts with some ICT, and of that 75 percent, it is assumed that 4 percent of the entities will have a reportable cyber incident for which this information collection activity applies.

Number of respondents:	2,821
Responses per respondent:	4
Total annual responses:	11,284
Hours per response:	4
Total burden hours:	45,136

(2) Preserving data resulting from data preservation activities and conducting data preservation activities.

It is estimated that this activity will take 7.5 hours to preserve data and conduct data preservation activities applied to 2,821 entities, of which 1,854 are small business entities, or 4 percent of the 75 percent of entities impacted by this portion of the proposed rule.

Number of respondents: 2,821
Responses per respondent: 1
Total annual responses: 2,821
Hours per response: 7.5
Total burden hours: 21,158

(3) Developing and maintaining customization files.

It is estimated that this activity will take 5 hours to develop and maintain customization files applied to 35,263 entities, of which 23,174, are small business entities, or 50 percent of the 75 percent of entities impacted by this portion of the proposed rule.

Number of respondents: 35,263
Responses per respondent: 1
Total annual responses: 35,263
Hours per response: 5
Total burden hours: 176,315

(4) Developing and providing a software bill of materials (SBOM), if required.

It is estimated that this activity will take 80 hours to develop and maintain an SBOM applied to 70,526 entities, of which 46,348 are small business entities, or the 75 percent of entities impacted by this portion of the proposed rule.

Number of respondents: 70,526
Responses per respondent: 1
Total annual responses: 70,526
Hours per response: 80
Total burden hours: 5,642,080

(5) Providing incident and damage assessment information, if requested.

It is estimated that this activity will take 2 hours to submit the preserved data and images, the SBOM, if

requested, and the customization files applied to 564 entities, of which 371 are small business entities, or 20 percent of 4 percent of the 75 percent of entities impacted by this portion of the proposed rule.

Number of respondents:	564
Responses per respondent:	1
Total annual responses:	564
Hours per response:	2
Total burden hours:	1,128

(6) Providing malicious code samples or artifacts, if available.

It is estimated that this activity will take 0.5 hours to share the malicious code samples or artifacts, applied to 1,128 entities, of which 742 are small business entities, or 40 percent of 4 percent of the 75 percent of entities impacted by this portion of the proposed rule.

Number of respondents:	1,128
Responses per respondent:	1
Total annual responses:	1,128
Hours per response:	0.5
Total burden hours:	564

(7) Sharing threat indicator information.

It is estimated that this activity will take 1 hour per week to share the threat indicator information, or 52 hours per year, applied to 70,526 entities, of which 46,348 are small business entities to be shared via the Automated Indicator Sharing (AIS), of 75 percent of entities, which are impacted by this portion of the proposed rule.

Number of respondents:	70,526
Responses per respondent:	1
Total annual responses:	70,526
Hours per response:	52

Total burden hours: 3,667,352

(8) Developing a supplier's declaration of conformity (regarding IPv6) and providing, if required.

It is estimated that this activity will take 8 hours applied to 70,526 entities, of which 46,348 are small business entities, or 75 percent of entities impacted by this portion of the proposed rule.

Number of respondents:	70,526
Responses per respondent:	1
Total annual responses:	70,526
Hours per response:	8
Total burden hours:	564,208

(9) Developing and providing an IPv6 Implementation Plan, if required.

It is estimated that to develop and provide an IPv6 Implementation Plan, if required, will take 20 hours applied to 705 entities, of which 463 are small business entities, or 1 percent of 75 percent of entities impacted by this portion of the proposed rule.

Number of respondents:	705
Responses per respondent:	1
Total annual responses:	705
Hours per response:	20
Total burden hours:	14,100

The total public burden is below:

Number of respondents:	254,880
Responses per respondent:	1.0332
Total annual responses:	263,343
Hours per response:	38.47
Total hours:	10,132,040

B. Request for Comments Regarding Paperwork Burden.

Submit comments on this collection of information no later than **[INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]** through *https://www/regulations.gov* and follow the instructions on the site. All items submitted must cite OMB Control No. 9000-XXXX, Incident and Threat Reporting and Incident Response Requirements. Comments received generally will be posted without change to *https://www.regulations.gov*, including any personal and/or business confidential information provided. To confirm receipt of your comment(s), please check *https://www.regulations.gov*, approximately two to three days after submission to verify posting. If there are difficulties submitting comments, contact the GSA Regulatory Secretariat Division at 202-501-4755 or *GSARegSec@gsa.gov*.

Public comments are particularly invited on:

- The necessity of this collection of information for the proper performance of the functions of Federal Government acquisitions, including whether the information will have practical utility;
- The accuracy of the estimate of the burden of this collection of information;
- Ways to enhance the quality, utility, and clarity of the information to be collected; and
- Ways to minimize the burden of the collection of information on respondents, including the use of

automated collection techniques or other forms of information technology.

Requesters may obtain a copy of the supporting statement from the General Services Administration, Regulatory Secretariat Division by calling 202-501-4755 or emailing *GSARegSec@gsa.gov*. Please cite OMB Control Number 9000-XXXX, Incident and Threat Reporting and Incident Response Requirements, in all correspondence.

List of Subjects in 48 CFR Parts 1, 2, 4, 7, 10, 11, 12, 39, and 52

Government procurement.

William F. Clark,
Director,
Office of Government-wide
Acquisition Policy,
Office of Acquisition Policy,
Office of Government-wide Policy.

Therefore, DoD, GSA, and NASA propose amending 48 CFR parts 1, 2, 4, 7, 10, 11, 12, 39, and 52 as set forth below:

1. The authority citation for 48 CFR parts 1, 2, 4, 7, 10, 11, 12, 39, and 52 continues to read as follows:

AUTHORITY: 40 U.S.C. 121(c); 10 U.S.C. chapter 4 and 10 U.S.C. chapter 137 legacy provisions (see 10 U.S.C. 3016); and 51 U.S.C. 20113.

PART 1—FEDERAL ACQUISITION REGULATIONS SYSTEM

2. In section 1.106 amend in the table following the introductory text, by adding in numerical order, entry for "52.239-ZZ" and its corresponding OMB Control Number "9000-XXXX" to read as follows.

1.106 OMB approval under the Paperwork Reduction Act.

* * * * *

FAR Segment	**OMB Control Number**
* * * * * * *	
52.239-ZZ	9000-XXXX
* * * * * * *	

* * * * *

PART 2—DEFINITIONS OF WORDS AND TERMS

3. Amend section 2.101 in paragraph (b)(2) by—

a. Removing the definition "Information and communication technology (ICT)"; and adding the definition "Information and communications technology (ICT)" in its place; and

b. Adding in alphabetical order the definitions "Information system", "Internet of Things (IoT) devices", "Operational technology", "Telecommunications equipment", and "Telecommunications services".

The revision and additions read as follows:

2.101 Definitions.

* * * * *

(b) * * *

(2) * * *

Information and communications technology (ICT) means information technology and other equipment, systems, technologies, or processes, for which the principal function is the creation, manipulation, storage, display, receipt, or transmission of electronic data and information, as well as any associated content. Examples of ICT include but are not limited to the following: Computers and peripheral equipment; information kiosks and transaction machines; telecommunications equipment; telecommunications services; customer premises equipment; multifunction office machines; computer software; applications; websites; electronic media; electronic documents; Internet of Things (IoT) devices; and operational technology.

* * * * *

Information system means a discrete set of information resources organized for the collection, processing,

maintenance, use, sharing, dissemination, or disposition of information (44 U.S.C. 3502(8)). Information resources, as used in this definition, includes any ICT.

* * * * *

Internet of Things (IoT) *devices* means, consistent with section 2 paragraph 4 of Pub. L. 116-207, devices that—

(1) Have at least one transducer (sensor or actuator) for interacting directly with the physical world, have at least one network interface, and are not conventional information technology devices, such as smartphones and laptops, for which the identification and implementation of cybersecurity features is already well understood; and

(2) Can function on their own and are not only able to function when acting as a component of another device, such as a processor.

* * * * *

Operational technology means programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems or devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples of operational technology include industrial control systems, building management systems, fire control systems, and physical access control mechanisms (NIST SP 800-160 vol 2).

* * * * *

Telecommunications equipment means equipment used to transmit, emit, or receive signals, signs, writing, images, sounds, or intelligence of any nature, by wire, cable, satellite, fiber optics, laser, radio, or any other electronic, electric, electromagnetic, or acoustically coupled means.

Telecommunications services means services used to transmit, emit, or receive signals, signs, writing, images, sounds, or intelligence of any nature, by wire, cable, satellite, fiber optics, laser, radio, or any other electronic, electric, electromagnetic, or acoustically coupled means.

* * * * *

PART 4—ADMINISTRATIVE AND INFORMATION MATTERS

4. Amend section 4.1202 by adding paragraph (a)(35) to read as follows:

4.1202 Solicitation provision and contract clause.

(a) * * *

(35) 52.239-AA, Security Incident Reporting Representation.

* * * * *

4.1901 [Amended]

5. Amend section 4.1901 by removing the definition "Information system".

PART 7—ACQUISITION PLANNING

7.103 [Amended]

6. Amend section 7.103 by removing from paragraph (q) "information and communication technology" and adding "information and communications technology" in its place.

7. Amend section 7.105 by revising paragraph (b)(5)(iii) to read as follows:

7.105 Contents of written acquisition plans.

* * * * *

(b) * * *

(5) * * *

(iii) For ICT acquisitions using Internet Protocol, discuss whether the requirements documents include the Internet Protocol Version 6 (IPv6) requirements specified in 39.106-1 or a waiver of these requirements has been granted by the agency's Chief Information Officer in accordance with 39.106-2.

* * * * *

PART 10-MARKET RESEARCH

10.001 [Amended]

8. Amend section 10.001 by removing from paragraph (a)(3)(ix) "information and communication technology" and adding "information and communications technology" in its place.

PART 11—DESCRIBING AGENCY NEEDS

9. Amend section 11.002 by—

a. Removing from paragraph (f)(1)(i) ”information and communication technology” and adding “information and communications technology” in its place; and

b. Revising paragraph (g).

The revision reads as follows:

11.002 Policy.

* * * * *

(g) For information on Internet Protocol Version 6 (IPv6) see 39.106.

* * * * *

PART 12—ACQUISITION OF COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES

10. Amend section 12.202 by—

a. Removing from paragraph (d) “information and communication technology” and adding “information and communications technology” in its place; and

b. revising paragraph (e).

The revision reads as follows:

12.202 Market research and description of agency need.

* * * * *

(e) When acquiring information technology using Internet Protocol, agencies must include the appropriate Internet Protocol version 6 (IPv6) compliance requirements in accordance with 39.106 and 39.108.

PART 39—ACQUISITION OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

11. The heading for part 39 is revised to read as set forth above.

12. Amend section 39.000 by revising paragraph (b) to read as follows:

39.000 Scope of part.

* * * * *

(b) Information and communications technology (ICT), as well as supplies and services that use ICT (see 2.101(b)).

13. Amend section 39.001 by revising the first sentence in paragraph (a), and paragraph (b) to read as follows:

39.001 Applicability.

* * * * *

(a) ICT, as well as supplies and services that use ICT, which includes information technology, Internet of Things (IoT) devices (e.g., connected appliances, wearables), and operational technology, by or for the use of agencies except for acquisitions of information technology for national security systems. * * *

(b) ICT by or for the use of agencies or for the use of the public. When applying the policy in subpart 39.2, see the exceptions at 39.204 and exemptions at 39.205.

14. Amend section 39.002 by adding in alphabetical order the definition "Supplier's declaration of conformity" to read as follows:

39.002 Definitions.

* * * * *

Supplier's declaration of conformity means a standardized format to document the USGv6 capabilities supported by a specific product or set of products and provides traceability back to the accredited laboratory that conducted the tests (see NIST SP 500-281B).

15. Amend section 39.101 by revising paragraph (d) to read as follows:

39.101 Policy.

* * * * *

(d) When acquiring information and communications technology (ICT) using Internet Protocol, agencies must include the appropriate Internet Protocol version 6 (IPv6) compliance requirements in accordance with 39.106.

* * * * *

16. Revise section 39.106 and add sections 39.107 and 39.108 to read as follows:

39.106 Internet Protocol version 6 (IPv6).

39.106-1 Policy.

ICT products and services must conform, at a minimum, to the IPv6 mandatory capabilities in the current version of the USGv6 Profile (National Institute of Standards and

Technology (NIST) SP 500-267B) or, if the agency Chief Information Officer (CIO) grants a waiver, provide for a product/service-specific IPv6 implementation plan (see 39.106-2(c)). See Office of Management and Budget (OMB) Memorandum M-21-07, Completing the Transition to Internet Protocol Version 6 (IPv6), dated November 19, 2020.

39.106-2 Waiver of IPv6 requirements.

(a) The agency's CIO may grant a waiver for any of the IPv6 mandatory capabilities specified in 39.106-1.

(b) The contracting officer shall coordinate with the requiring activity to verify if the agency CIO has waived any IPv6 mandatory capabilities, in accordance with agency procedures.

(c) If a waiver has been granted by the agency's CIO, the contracting officer shall include that fact in the solicitation and also include a request for documentation from offerors detailing explicit plans, including timelines, to incorporate the IPv6 mandatory capabilities in NIST SP 500-267B.

39.107 Response to incident reports and requests for information or access.

(a) If the contracting officer receives a notice of a request for access to contractor information or equipment from the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), or the contractor, the contracting officer shall—

(1) Acknowledge the request, though acknowledgment is not a required condition to trigger contractor response pursuant to clause 52.239-ZZ(c)(6);

(2) Facilitate the request, including through coordination, as appropriate, with the requiring activity, senior agency official for privacy, agency chief information security officer, agency legal counsel, and any other agency officials identified in the notification requirement;

(3) Document the contract file to reflect the access request and any access granted pursuant to the request; and

(4) If notified by CISA or the FBI that retention of records pursuant to paragraph (c)(1)(ii) of 52.239-ZZ is necessary beyond 180 days, the contracting officer shall instruct the contractor to retain such records as necessary.

(b) If the contracting officer receives a request from CISA, the agency CIO or Chief Information Security Officer, or the relevant program office for access to a software bill of materials as provided under paragraph (c)(3) of 52.239-ZZ, the contracting officer shall provide such access in a timely manner in accordance with agency procedures.

(c) If the contracting officer receives a notification that an incident report has been filed by a contractor

pursuant to paragraph (b)(1) of 52.239-ZZ, the contracting officer shall—

(1) Notify the requiring activity;

(2) If the affected contract is an indefinite delivery contract, notify any contracting officers that placed orders under the contract; and

(3) Follow any additional agency procedures.

39.108 Solicitation provision and contract clauses.

(a) The contracting officer shall insert a clause substantially the same as the clause at 52.239-1, Privacy or Security Safeguards, in solicitations and contracts for information technology that require security of information technology, and/or are for the design, development, or operation of a system of records using commercial information technology services or support services.

(b) The contracting officer shall insert the clause at 52.239-ZZ, Incident and Threat Reporting and Incident Response Requirements for Products or Services Containing Information and Communications Technology, in all solicitations and contracts.

(c) The contracting officer shall insert the provision at 52.239-AA, Security Incident Reporting Representation, in all solicitations.

17. The heading for subpart 39.2 is revised to read as follows:

Subpart 39.2—Information and Communications Technology Accessibility

39.201 [Amended]

18. Amend section 39.201 by removing from paragraph (a) "information and communication technology" and adding "information and communications technology" in its place.

PART 52—SOLICITATION PROVISIONS AND CONTRACT CLAUSES

19. Amend section 52.204-8 by revising the date of the clause and adding paragraph (c)(1)(xxvi) to read as follows:

52.204-8 Annual Representations and Certifications.

* * * * *

Annual Representations and Certifications (DATE)

* * * * *

(c)(1) * * *

(xxvi) 52.239-AA, Security Incident Reporting Representation. This provision applies to all solicitations.

* * * * *

20. Amend section 52.212-3 by—

a. Revising the date of the provision;

b. Removing from the introductory text "(c) through (v)" and adding "(c) through (w)" in its place;

c. In paragraph (a), adding in alphabetical order the definitions "Information and communications

technology", "Security incident", and "Security incident reports";

d. Removing from paragraph (b)(2) "*Offeror to identify the applicable paragraphs at (c) through (v)*" and adding "*Offeror to identify the applicable paragraphs at (c) through (w)*" in its place; and

e. Adding paragraph (w).

The revision and additions read as follows:

52.212-3 Offeror Representations and Certifications—Commercial Products and Commercial Services.

* * * * *

OFFEROR REPRESENTATIONS AND CERTIFICATIONS—COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES (DATE)

* * * * *

(a) * * *

Information and communications technology has the meaning given in paragraph (a) of FAR clause 52.239-ZZ, Incident and Threat Reporting and Incident Response Requirements for Products or Services Containing Information and Communications Technology.

* * * * *

Security incident has the meaning given in paragraph (a) of FAR clause 52.239-ZZ.

Security incident reports means the submission of information on security incidents as required by paragraphs (b)(1) through (b)(3) of FAR clause 52.239-ZZ.

* * * * *

(w) *Security Incident Reporting Representation.*

(1) The Offeror represents that it has submitted in a current, accurate, and complete manner, all security incident reports required by current existing contracts between the Offeror and the Government.

(2) Under current existing contracts between the Offeror and the Government where information and communications technology is used or provided in the performance of a subcontract, the Offeror represents that it has required each first tier subcontractor to:

(i) Notify the Offeror within 8 hours of discovery of a security incident, as required by paragraph (f) of FAR clause 52.239-ZZ; and

(ii) Require the next lower tier subcontractor to include the requirement to notify the prime Contractor and next higher tier subcontractor within 8 hours of discovery of a security incident, and include this reporting requirement and continued flow down requirement in any lower tier subcontracts, in this and other executive agency contracts, as required by paragraph (f) of FAR clause 52.239-ZZ.

* * * * *

21. Amend section 52.212-5 by—

a. Revising the date of the clause;

b. Redesignating paragraphs (b)(63) and (64) as paragraphs (b)(64) and (65), and adding a new paragraph (b)(63);

c. Redesignating paragraph (e)(1)(xxiv) as paragraph (e)(1)(xxv), and adding a new paragraph (e)(1)(xxiv);

d. In Alternate II:

i. Revising the date of Alternate II; and

ii. Redesignating paragraph (e)(1)(ii)(W) as paragraph (e)(1)(ii)(X), and adding a new paragraph (e)(1)(ii)(W).

The revisions and additions read as follows:

52.212-5 Contract Terms and Conditions Required To Implement Statutes or Executive Orders—Commercial Products and Commercial Services.

* * * * *

CONTRACT TERMS AND CONDITIONS REQUIRED TO IMPLEMENT STATUTES OR EXECUTIVE ORDERS—COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES (DATE)

* * * * *

(b) * * *

__ (63) 52.239-ZZ, Incident and Threat Reporting and Incident Response Requirements for Products or Services Containing Information and Communications Technology (DATE) (E.O. 14028).

* * * * *

(e)(1) * * *

(xxiv) 52.239-ZZ, Incident and Threat Reporting and Incident Response Requirements for Products or Services Containing Information and Communications Technology (DATE) (E.O. 14028). Flow down required in accordance with paragraph (f) of FAR clause 52.239-ZZ.

* * * * *

Alternate II (DATE) * * *

* * * * *

(e)(1) * * *

(ii) * * *

(W) 52.239-ZZ, Incident and Threat Reporting and Incident Response Requirements for Products or Services Containing Information and Communications Technology (DATE) (E.O. 14028). Flow down required in accordance with paragraph (f) of FAR clause 52.239-ZZ.

22. Amend section 52.213-4 by—

a. Revising the date of the clause;

b. Removing from paragraph (a)(2)(vii) "(SEP 2023)" and adding "(DATE)" in its place; and

c. Redesignating paragraph (b)(1)(xxi) as paragraph (b)(1)(xxii) and adding a new paragraph (b)(1)(xxi).

The revision and addition read as follows:

52.213-4 Terms and Conditions—Simplified Acquisitions (Other Than Commercial Products and Commercial Services).

* * * * *

TERMS AND CONDITIONS—SIMPLIFIED ACQUISITIONS (OTHER THAN COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES) (DATE)

* * * * *

(b) * * *

(1) * * *

(xxi) 52.239-ZZ, Incident and Threat Reporting and Incident Response Requirements for Products or Services Containing Information and Communications Technology (DATE) (E.O. 14028). (Applies to all solicitations and contracts.)

* * * * *

52.239-1 [Amended]

23. Amend section 52.239-1 by removing from the introductory text "39.106" and adding "39.108(a)" in its place.

24. Add sections 52.239-AA and 52.239-ZZ to read as follows:

52.239-AA Security Incident Reporting Representation.

As prescribed in 39.108(c), insert the following provision:

SECURITY INCIDENT REPORTING REPRESENTATION (DATE)

(a) *Definitions*. As used in this provision: *Information and communications technology*, and *Security incident* have the meanings given in paragraph (a) of FAR clause 52.239-ZZ, Incident and Threat Reporting and Incident Response Requirements for Products or Services Containing Information and Communications Technology.

Security incident reports means the submission of information on security incidents as required by paragraphs (b)(1) through (b)(3) of FAR clause 52.239-ZZ.

(b) *Representation*.

(1) The Offeror represents that it has submitted in a current, accurate, and complete manner, all security incident reports required by current existing contracts between the Offeror and the Government.

(2) Under current existing contracts containing FAR clause 52.239-ZZ between the Offeror and the Government where information and communications technology is used or provided in the performance of a subcontract, the Offeror represents that it has required each first tier subcontractor to—

(i) Notify the Offeror within 8 hours of discovery of a security incident, as required by paragraph (f) of FAR clause 52.239-ZZ; and

(ii) Require the next lower tier subcontractor to include the requirement to notify the prime Contractor and next higher tier subcontractor within 8 hours of discovery of a security incident, and include this reporting requirement and continued flow down requirement in any lower tier subcontracts, in this and other executive agency contracts, as required by paragraph (f) of FAR clause 52.239-ZZ.

(End of provision)

52.239-ZZ Incident and Threat Reporting and Incident Response Requirements for Products or Services Containing Information and Communications Technology.

As prescribed in 39.108(b), insert the following clause:

INCIDENT AND THREAT REPORTING AND INCIDENT RESPONSE REQUIREMENTS FOR PRODUCTS OR SERVICES CONTAINING INFORMATION AND COMMUNICATIONS TECHNOLOGY (DATE)

(a) Definitions. As used in this clause –

Active storage means storing data in a manner that facilitates frequent use and ease of access.

Cold data storage means storing data in a manner that minimizes costs while still allowing some level of access and use.

Computer software

(1) Means -

(i) Computer programs that comprise a series of instructions, rules, routines, or statements, regardless of the media in which recorded, that allow or cause a computer to perform a specific operation or series of operations; and

(ii) Recorded information comprising source code listings, design details, algorithms, processes, flow charts, formulas, and related material that would enable the computer program to be produced, created, or compiled.

(2) Does not include computer databases or computer software documentation.

Cyber threat indicators, in accordance with 6 U.S.C. 1501, means information that is necessary to describe or identify—

(1) Malicious reconnaissance, including anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or security vulnerability;

(2) A method of defeating a security control or exploitation of a security vulnerability;

(3) A security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability;

(4) A method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability;

(5) Malicious cyber command and control;

(6) The actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat;

(7) Any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law; or

(8) Any combination thereof.

Defensive measures means an action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability. The term "defensive measures" does not include a measure that destroys, renders unusable, provides unauthorized access to, or substantially harms an information system or information stored on, processed by, or transiting such information system not owned by the private entity operating the measure; or by another entity or Federal entity that is authorized to provide consent and has provided consent to that private entity for operation of such measure (6 U.S.C. 1501(7)).

Eradication means eliminating or resolving the mechanisms, components, and cause(s) of the incident, (such as deleting malware and disabling breached user accounts), as well as identifying all affected hosts within information systems and mitigating all exploited vulnerabilities.

Event means any observable occurrence in a system or network.

Full access means, for all contractor information systems used in performance, or which support performance, of the contract—

(1) Physical and electronic access to—

(i) Contractor networks,

(ii) Systems,

(iii) Accounts dedicated to Government systems,

(iv) Other infrastructure housed on the same computer network,

(v) Other infrastructure with a shared identity boundary or interconnection to the Government system; and

(2) Provision of all requested Government data or Government-related data, including—

(i) Images,

(ii) Log files,

(iii) Event information, and

(iv) Statements, written or audio, of contractor employees describing what they witnessed or experienced in connection with the contractor's performance of the contract.

Government-related data means any information, document, media, or machine-readable material regardless of physical form or characteristics that is created or obtained by a contractor through the storage, processing, or communication of Government data. Government-related data does not include—

(1) A contractor's business records (e.g., financial records, legal records) that do not incorporate Government data, or

(2) Data such as operating procedures, software coding or algorithms that are not uniquely applied to the Government data.

Information and communications technology (ICT) means information technology and other equipment, systems, technologies, or processes, for which the principal function is the creation, manipulation, storage, display, receipt, or transmission of electronic data and information, as well as any associated content. Examples of ICT include but are not limited to the following: Computers and peripheral equipment; information kiosks and transaction machines; telecommunications equipment; telecommunications services; customer premises equipment; multifunction office machines; computer software; applications; websites; electronic media; electronic documents; internet of things (IoT) devices; and operational technology.

Information system means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (44 U.S.C. 3502(8)). Information resources, as used in this definition, includes any ICT.

Operational technology means programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems or devices detect or cause a direct change through the monitoring and or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms (NIST SP 800-160).

Security incident means actual or potential occurrence of the following-

(1) Any event or series of events, which pose(s) actual or imminent jeopardy, without lawful authority, to the integrity, confidentiality, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies;

(2) Any malicious computer software discovered on an information system; or

(3) Transfer of classified or controlled unclassified information onto an information system not accredited (i.e., authorized) for the appropriate security level.

Software bill of materials (SBOM) means a formal record containing the details and supply chain relationships of various components used in building software.

Supplier's declaration of conformity means a standardized format to document the USGv6 capabilities supported by a specific product or set of products and provides traceability back to the accredited laboratory that conducted the tests (see NIST SP 500-281B).

Telecommunications equipment means equipment used to transmit, emit, or receive signals, signs, writing, images, sounds, or intelligence of any nature, by wire, cable, satellite, fiber optics, laser, radio, or any other electronic, electric, electromagnetic, or acoustically coupled means.

Telecommunications services means services used to transmit, emit, or receive signals, signs, writing, images, sounds, or intelligence of any nature, by wire, cable, satellite, fiber optics, laser, radio, or any other electronic, electric, electromagnetic, or acoustically coupled means.

Telemetry means the automatic recording and transmission of data from remote or inaccessible sources to an information system in a different location for monitoring and analysis. Telemetry data may be relayed using radio, infrared ultrasonic, cellular, satellite or cable, depending on the application.

(b) *Security incident reporting*.

(1)(i) The Contractor shall submit a CISA Incident Reporting Form on all security incidents involving a

product or service provided to the Government that includes information and communications technology, or the information system used in developing or providing the product or service, to the Cybersecurity and Infrastructure Security Agency (CISA) in the Department of Homeland Security using the CISA Incident Reporting System. The CISA Incident Reporting System, along with information on types of incidents, can be found here: *https://www.cisa.gov/report*.

(ii) Consistent with applicable laws, regulations, and Governmentwide policies, CISA will share the information reported with any contracting agency potentially affected by the incident or by a vulnerability revealed by the incident and other executive agencies responsible for investigating or remediating cyber incidents, such as the Federal Bureau of Investigation (FBI), and other elements of the intelligence community.

(2) The Contractor shall also notify the Contracting Officer, and the contracting officer (or ordering officer) of any agency which placed an affected order under this contract, that an incident reporting portal has been submitted to CISA.

(3) The Contractor shall immediately and thoroughly investigate all indicators that a security incident may have occurred and submit information using the CISA incident reporting portal pursuant to paragraphs (b) and

(c) of this clause within 8 hours of discovery that a security incident may have occurred and shall update the submission every 72 hours thereafter until the Contractor, the agency, and/or any investigating agencies have completed all eradication or remediation activities. Security incidents involving specific types of information (e.g., controlled unclassified information, classified information) may require additional reporting that is separate from the requirements of this clause.

(4) In the event the Contractor suspects a compromise of a communications or messaging platform, the Contractor should avoid use of such potentially compromised means to provide notification(s) or otherwise communicate information about a security incident and associated response activities.

(c) *Supporting incident response.*

(1) *Data preservation and protection.*

(i) The Contractor shall collect, and preserve for at least 12 months in active storage followed by 6 months in active or cold storage, available data and information relevant to security incident prevention, detection, response and investigation within information systems used in developing or providing ICT products or services to the Government. This data includes, but is not limited to, network traffic data, full network flow, full packet capture, perimeter defense logs (firewall, intrusion

detection systems, intrusion prevention systems), telemetry, and system logs including, but not limited to, system event logs, authentication logs, and audit logs. Upon request by the Contracting Officer, the Contractor shall promptly provide this data and information to the Government.

(ii) When the Contractor has discovered that a security incident may have occurred on an affected information system, the Contractor shall immediately preserve and protect images of all known affected information systems and all available monitoring/packet capture data. Following submission of a security incident report pursuant to paragraph (b) of this clause, or receipt of a request for access pursuant to paragraph (c)(6) of this clause, such images and data shall be retained for the longer of—

(A) 180 days from the submission of the report or receipt of the request;

(B) Any longer period required under paragraph (c)(1)(i) of this clause; or

(C) If instructed to retain such images and data beyond 180 days by the Contracting Officer, until the Contractor is notified by the Contracting Officer that retention is no longer required.

(2) *Customization files.* The Contractor shall develop, store, and maintain throughout the life of the

contract and for at least 1 year thereafter an up-to-date collection of customizations that differ from manufacturer defaults on devices, computer software, applications, and services, which includes but is not limited to configuration files, logic files and settings on web and cloud applications for all information systems used in developing or providing an ICT product or service to the Government. Upon request by the Contracting Officer, or consistent with paragraph (c)(6) of this clause, the Contractor shall provide the cognizant program office/requiring activity, CISA and/or the FBI, with a copy of the current and historical customization files, and notice to the Contracting Officer that such information has been shared and with whom it has been shared.

(3) *Software bill of materials (SBOM).*

(i) The Contractor shall maintain, and upon the initial use of such software in the performance of this contract, provide or provide access to the Contracting Officer a current SBOM for each piece of computer software used in performance of the contract. Each SBOM shall be produced in a machine-readable, industry-standard format and shall comply with all of the minimum elements identified in Section IV of The Minimum Elements for a Software Bill of Materials (the current version at the time of solicitation) published by the Department of Commerce at *https://www.ntia.doc.gov/report/2021/minimum-elements-*

software-bill-materials-sbom, except for frequency which is addressed in paragraph (c)(3)(ii) of this clause. These minimum elements establish the baseline technology and practices for the provisioning of a SBOM that enable computer software transparency, capturing both the technology and functional operation.

(ii) If a piece of computer software used in the performance of the contract is updated with a new build or major release, the contractor must update the computer SBOM in paragraph (c)(3)(i) of this clause to reflect the new version of the computer software and provide (or provide access to) the updated SBOM to the Contracting Officer. This includes computer software builds to integrate an updated component or dependency.

(iii) If an SBOM has been provided to the contracting officer at the basic contract level, the SBOM does not need to be provided to the contracting officer for each order.

(4) *Incident and damage assessment activities.* If the Government elects to conduct an incident or damage assessment regarding a security incident, the Contractor shall promptly provide to the Government, and any independent third party specifically authorized by the Government, all information identified in paragraphs (c)(1), (c)(2), and (c)(3) of this clause.

(5) *Malicious computer software.* If the Contractor discovers and isolates malicious computer software in connection with a security incident, the Contractor shall submit malicious code samples or artifacts to CISA using the appropriate form at *https://www.malware.us-cert.gov* within 8 hours of discovery and isolation of the malicious computer software in addition to required incident reporting pursuant to paragraph (b) of this clause.

(6) *Access, including access to additional information or equipment necessary for forensic analysis.*

(i) Upon request by the Contracting Officer, CISA or the FBI, in response to a security incident reported in accordance with paragraph (b)(1) of this clause, or in response to a CISA or FBI access request based on an identified security incident, the Contractor shall first validate any CISA or FBI access request according to the procedures in (c)(6)(ii) of this clause, and then respond to any requests for access from the contracting agency, CISA, and the FBI within 96 hours with available information identified in paragraphs (c)(1), (c)(2), and (c)(3) of this clause, as well as access to additional information or equipment that is necessary to conduct a forensic analysis.

(A) Consistent with applicable laws, regulations, and Governmentwide policies that limit or prohibit access to data, this includes full access and

cooperation for all activities determined by the contracting agency, CISA, and the FBI to:

(*1*) Ensure an effective incident response, investigation of potential incidents, and threat hunting activity, including supporting cloud and virtual infrastructure; and

(*2*) Coordinate with CISA, the FBI, and the contracting agency to develop and implement corrections, fixes or other mitigations for discovered vulnerabilities and exploits.

(B) This also includes timely access to Contractor personnel involved in the performance of the contract.

(ii) Prior to responding to a request from CISA or the FBI for information or access under this clause, the Contractor shall:

(A)(*1*) For requests from CISA, confirm the validity of the request by contacting CISA Central at *report@cisa.gov* or (888) 282-0870,

(*2*) For requests from the FBI, confirm the validity of the request by contacting the FBI field office identified by the requestor using contact information from *https://www.fbi.gov/contact-us/field-offices*; and

(B) Immediately notify the Contracting Officer and any other agency official designated in the contract in writing of receipt of the request. Provision of information

and access to CISA and the FBI under this clause shall not be delayed by submission of this notification or awaiting acknowledgement of its receipt.

(d) *Cyber threat indicators and defensive measures reporting.* The Contractor shall either-

(1) Subscribe to the Automated Indicator Sharing (AIS) (*https://www.cisa.gov/ais*) capability or successor technology during the performance of the contract. The Contractor shall share cyber threat indicators and recommended defensive measures, to include associated tactics, techniques, and procedures, if available, when such indicators or measures are observed on information and communications technology used in performance of the contract or provided to the Government, in an automated fashion using this medium during the performance of the contract. Contractors submitting cyber threat indicators and defensive measures through AIS will receive applicable legal protections (see 6 U.S.C. 1505) in accordance with the Cybersecurity Information Sharing Act of 2015, Procedures and Guidance; or

(2) During the performance of the contract, participate in an information sharing and analysis organization or information sharing and analysis center with the capability to share indicators with AIS or successor technology and that further shares cyber threat indicators and recommended defensive measures submitted to

it with AIS, during the performance of the contract. The Contractor shall share cyber threat indicators and recommended defensive measures, when such indicators or measures are observed on information and communications technology used during performance of the contract or provided to the Government, with the ISAO or ISAC during the performance of the contract, in addition to required incident reporting pursuant to paragraph (b) of this clause. Contractors submitting cyber threat indicators and defensive measures through an ISAO or ISAC will receive applicable legal protections in accordance with the Cybersecurity Information Sharing Act of 2015 Procedures and Guidance.

(e) *Internet Protocol version 6 (IPv6).*

(1) This paragraph (e) applies to—

(i) Any ICT using internet protocol provided to the Government, and

(ii) Any interfaces exposed to the Government from a Contractor information system using internet protocol.

(2) The Contractor shall comply with all applicable mandatory capabilities specified in the current version of the USGv6 Profile (NIST Special Publication 500-267B) (see Office of Management and Budget (OMB) Memorandum M-21-07, Completing the Transition to Internet Protocol Version 6 (IPv6) dated November 19, 2020) and provide to the

Contracting Officer a copy of or access to the corresponding supplier's declaration of conformity in accordance with the USGv6 Test Program (see NIST SP 500-281A).

(3) The agency may have granted a waiver to this paragraph (e). If so, elsewhere in this contract the waiver will be identified along with any conditions (see FAR 39.106-2).

(f) *Subcontracts.* The Contractor shall include the substance of this clause, including this paragraph (f), in all subcontracts where ICT is used or provided in the performance of the subcontract, including subcontracts for the acquisition of commercial products or services. All references to the Contractor are applicable to all subcontractors. The Contractor shall require subcontractors to notify the prime Contractor and next higher tier subcontractor within 8 hours of discovery of a security incident.

(End of clause)

25. Amend section 52.244-6 by—

a. Revising the date of the clause; and

b. Redesignating paragraph (c)(1)(xxi) as paragraph (c)(1)(xxii) and adding a new paragraph (c)(1)(xxi).

The revision and addition read as follows:

52.244-6 Subcontracts for Commercial Products and Commercial Services.

* * * * *

SUBCONTRACTS FOR COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES (DATE)

* * * * *

(c)(1) * * *

(xxi) 52.239-ZZ, Incident and Threat Reporting and Incident Response Requirements for Products or Services Containing Information and Communications Technology (Date) (E.O. 14028), if flow down is required in accordance with paragraph (f) of FAR clause 52.239-ZZ.

* * * * *

[FR Doc. 2023-21328 Filed: 10/2/2023 8:45 am; Publication Date: 10/3/2023]