)-EP

DEPARTMENT OF DEFENSE

GENERAL SERVICES ADMINISTRATION

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

48 CFR Parts 1, 2, 4, 7, 10, 11, 12, 37, 39 and 52

[FAR Case 2021-019; Docket No. FAR-2021-0019; Sequence No. 1]

RIN 9000-AO35

Federal Acquisition Regulation: Standardizing Cybersecurity Requirements for Unclassified Federal Information Systems

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 to standardize cybersecurity contractual requirements across Federal agencies for unclassified Federal information systems, and a statute on improving the Nation's cybersecurity.

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 2021-019 to the Federal eRulemaking portal at *https://www.regulations.gov* by searching for "FAR Case 2021-019". Select the link "Comment Now" that corresponds with "FAR Case 2021-019". Follow the instructions provided on the "Comment Now" screen. Please include your name, company name (if any), and "FAR Case 2021-019" 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 2021-019" 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 three days after submission to verify posting.

FOR FURTHER INFORMATION CONTACT: For clarification of content, contact Ms. Carrie Moore, Procurement Analyst, at (571) 300-5917 or by email at *carrie.moore@gsa.gov*. For information pertaining to status, publication schedules, or

alternative 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 2021-019.

SUPPLEMENTARY INFORMATION:

I. Background

DoD, GSA, and NASA are proposing to revise the FAR to provide standardized cybersecurity contractual requirements across Federal agencies for Federal information systems (FIS) by implementing: (1) recommendations received in accordance with paragraph (i) of section 2 of Executive Order (E.O.) 14028, "Improving the Nation's Cybersecurity," dated May 12, 2021; and (2) paragraphs (a) and (b)(1) of section 7 of the Internet of Things (IoT) Cybersecurity Improvement Act of 2020 (Pub. L. 116-207). Other aspects of section 2 of E.O. 14028 are being implemented in FAR Case 2021-017, Cyber Threat and Incident Reporting and Information Sharing. This rulemaking does not implement Office of Management and Budget Memorandum M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices, issued September 14, 2022.

The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public and private sectors' security and privacy. The Council of Economic Advisors estimates that malicious cyber

activity cost the U.S. economy between $57 billion and $109 billion in 2016. With threats continuing to grow, this activity could yield costs of more than $1 trillion over a decade. In addition to the aggregate effect on the economy, the impact of a single cyber incident to an individual company can be crippling. An October 2020 study from the Cybersecurity and Infrastructure Security Agency (CISA) in the Department of Homeland Security (DHS), entitled "Cost of a Cyber Incident: Systematic Review and Cross-Validation," indicates that the average per-incident cost to small businesses of less than 250 employees and medium-sized businesses of at least 250 employees, but less than 1,000 employees, could range from $5,000 to $226,000, and from $102,000 to $40 million for large businesses of 1,000 employees or more.

The Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions. Contractors must be able to adapt to the continuously changing threat environment, ensure products are built and operate securely, and coordinate with the Government to foster a more secure cyberspace. It also is essential that the Government - and its contractors - take a coordinated approach to complying with applicable security and privacy requirements, which are closely related, though they come from independent and separate disciplines. In the end, the trust the United States

places in its digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is, and to the consequences it will incur if that trust is misplaced.

The Government has a responsibility to protect and secure its computer systems, whether they are cloud-based, on-premises, or a hybrid of the two. The scope of that protection and security must encompass the systems that process data (e.g., information technology (IT)) and those that run the vital machinery that ensures its safety (e.g., operational technology (OT)). The Government contracts with IT and OT service providers to conduct an array of day-to-day functions on Federal Information Systems (FIS).

A FIS is an information system used or operated by an agency, by a contractor of an agency, or by another organization, on behalf of an agency. All FISs require protection as part of good risk management practices. Agencies are responsible for determining what information systems are FIS, in accordance with the definition provided in this rule.

Currently, contractual requirements for the cybersecurity standards of unclassified FISs are largely based on agency-specific policies and regulations. The risks associated with agency-specific policies can result in inconsistent security requirements across contracts, as well as be unclear, add costs, and restrict competition.

To address these risks, paragraph (i) of section 2 of E.O 14028 requires the DHS Secretary, acting through the Director of CISA, to review agency-specific cybersecurity requirements that currently exist as a matter of law, policy, or contract and recommend to the FAR Council standardized contract language for appropriate cybersecurity requirements. Paragraph (j) of section 2 of E.O. 14028 then directs that FAR Council to consider the contract language received from DHS and publish for public comment any proposed updates to the FAR. This proposed rule would implement the DHS recommendations across all Federal agencies to streamline requirements and improve compliance for contractors and the Government.

By standardizing a set of minimum cybersecurity standards to be applied consistently to FISs, the proposed rule would ensure that such systems are better positioned in advance to protect from cyber threats. In addition, and as required by paragraph (k) of section 2 of E.O. 14028, upon issuance of a final rule, agencies shall update their agency-specific requirements to remove any requirements that are duplicative of such FAR updates.

II. Discussion and Analysis

This proposed rule provides cybersecurity policies, procedures, and requirements for contractor services to develop, implement, operate, or maintain a FIS. This rule underscores that compliance with these requirements is

material to eligibility and payment under Government contracts.

A contract to develop, implement, operate, or maintain a FIS may require contractors to utilize cloud computing services, services other than cloud computing services (i.e., non-cloud computing services, also known as on-premises computing services), or a hybrid of both approaches when providing services under the contract. As such, this rule specifies the policies, procedures, and requirements that apply to each service approach (i.e., a FIS that uses non-cloud computing services and a FIS that uses cloud computing services). When an acquisition requires the use of both non-cloud computing services and cloud computing services in performance of the contract, the rule would require compliance with the policies, procedures, and requirements for each service approach, as they respectively apply to the FIS.

This rule proposes to: (1) add a new FAR subpart 39.X, "Federal Information Systems," to prescribe policies and procedures for agencies when acquiring services to develop, implement, operate, or maintain a FIS; (2) add and revise definitions in parts 2 and 39.X using current language from statute, regulation, Office of Management and Budget memoranda and circulars, and National Institute of Standards and Technology (NIST) Special Publications (SP) guidance; (3) make conforming changes to parts 4, 7, 37,

and 39 to further implement policies and procedures described below; and (4) add two new FAR clauses to be used in contracts for services to develop, implement, operate, or maintain a FIS: FAR clause 52.239-YY, "Federal Information Systems Using Non-Cloud Computing Services," which is included in solicitations and contracts that use non-cloud computing services in performance of the contract; and FAR clause 52.239-XX, "Federal Information Systems Using Cloud Computing Services," which is included in solicitations and contracts that use cloud computing services in performance of the contract. The policies and requirements specified in this rule are discussed below.

A. FISs using non-cloud computing services.

FIPS Publication 199 Impact Level and Mandatory Security and Privacy Controls. As each requirement will vary in scope, as well as the function of each FIS, adequate security and privacy controls must be identified when agencies define their acquisition requirements. Agencies will use Federal Information Processing Standard (FIPS) Publication 199 to categorize the FIS based on its impact analysis of the information processed, stored, or transmitted by the system. As a result of the analysis, the FIPS Publication 199 impact level of the FIS, as well as a set of necessary security and privacy controls for the FIS, will be specified by the agency in the contract. As part of the security and privacy controls identified by the

agency, the rule would require agencies to address multifactor authentication, administrative accounts, consent banners, Internet of Things device controls, and assessment requirements, when applicable, in every applicable contract. The proposed rule adds text to FAR part 7 to ensure that acquisition planners develop agency requirements in accordance with the rule's requirements.

Records Management and Government Access. To assist the Government: (1) in carrying out a program of inspection to safeguard against threats and hazards to the security and privacy of Government data, or (2) for the purpose of audits, investigations, inspections or similar activities, paragraph (c) of the clause 52.239-YY would require contractors to provide the Government's authorized representatives, which includes CISA (for civilian agencies) as well as other Federal agencies as specified by the contracting officer, with timely and full access to Government data and Government-related data, timely access to contractor personnel involved in performance of the contract, and specifically for the purpose of audit, investigation, inspection, or other similar activity, physical access to any contractor facility with Government data including any associated metadata. If the contractor receives a request for access from CISA, the contractor must confirm the validity of the request by contacting CISA

and notifying the contracting officer in writing of the request for access.

Assessments. When a FIS is designated as a moderate or high FIPS Publication 199 impact level, paragraph (d) of the clause 52.239-YY would require contractors: (1) to conduct, at least annually, a cyber threat hunting and vulnerability assessment to search for vulnerabilities, risks, and indicators of compromise; and (2) to perform to an annual, independent assessment of the security of each FIS. Upon completion, contractors would submit the results of an assessment, including any recommended improvements or risk mitigations, to the contracting officer. The agency will review the results of the assessment. The agency may require the contractor to implement the recommended improvement or mitigation. The agency may provide the contractor with a rationale for not requiring the contractor to implement the recommendation or mitigation, and if so, the contractor would document the agency's rationale in the System Security Plan (SSP).

If the contractor contracts with a third-party assessment organization to perform these assessments, contractors must enter into a confidentiality agreement with the organization to protect Federal data under the contract. To assist with mitigating any potential conflicts of interest, the clause would also require contractors to notify the contracting officer of any

existing business relationships the contractor may have with the organization.

Specification of Additional Security and Privacy Controls. Agencies will also specify in the requirement the security and privacy controls necessary for contract performance. In accordance with paragraph (e) of the clause 52.239-YY, the controls specified by the agency will be based on the current version of the following documents at the time of contract award: NIST SP 800-53, "Security and Privacy Controls for Information Systems and Organizations;" NIST SP 800-213 "IOT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements;" NIST SP 800-161, "Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations;" and NIST SP 800-82, "Guide to Industrial Control Systems Security." Paragraph (e) also requires contractors to: (1) develop, review, and update, if appropriate, an SSP to support authorization of all applicable FIS, and (2) have contingency plans for all information technology systems, aligned to NIST SP 800-34, "Contingency Planning Guide for Federal Information Systems." The rule does not require a specific format for the SSP, but NIST SP 800-34 provides information on a template that contractors may choose to use. Contractors will be expected to provide a copy of the SSP, as well as

make contingency plans available, to an agency upon request.

In some situations, an information system may be designated as a high value asset by the agency. In accordance with paragraph (e) of the clause 52.239-YY, contractors will be subject to, as specified in the requirement, additional security and privacy controls for a high value asset, that could include the implementation of a high value asset overlay, immediate failover and/or recover plans, and complying with requisite cybersecurity assessments (e.g., contractor cooperation and allowing access).

Additional considerations. For each non-cloud FIS developed, implemented, operated, or maintained, paragraph (f) of the clause 52.239-YY requires contractors to apply NIST SP guidance on various topics when performing or managing certain activities related to the FIS, including: managing information system risk when supporting agency risk management activities; developing risk management processes; conducting and communicating the results of risk assessments; designing zero trust architecture approaches; considering security when executing within the context of systems engineering; selecting, adapting, and using cyber resiliency constructs for new systems, system upgrades, or repurposed systems; implementing continuous monitoring strategies for FISs; and implementing digital identity

services and requirements. Further, paragraph (f)(7) requires contractors to provide the Government with a copy of their continuous monitoring strategy for the FIS that demonstrates an ongoing awareness of information security, vulnerabilities, and threats in order to support risk management decisions, and applies the use of automation, wherever possible; protects vulnerability scan data, logs, and telemetry; and applies the guidance of NIST SP 800-137, "Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations."

Cyber supply chain risk management. Paragraph (g) of the clause 52.239-YY advises that contractors may implement alternative, additional, or compensating cyber supply chain risk management security controls from those stated in the contract, when authorized in writing to do so by the contracting officer.

Notifiable incident reporting, incident response, and threat reporting. Paragraph (h) of the clause 52.239-YY reminds contractors that they must refer to FAR clause 52.239-ZZ, "Incident and Threat Reporting and Incident Response Requirements for Products or Services Containing Information and Communications Technology" (see FAR case 2021-017), for guidance on handling security incident and cyber threat reporting.

Other protections. Paragraph (i) of the clause 52.239-YY specifies the limitations on contractor access

to, use, and disclosure of Government data, Government-related data, and metadata under the contract, and requires contractors to notify the contracting officer of any requests from an entity other than the contracting activity (including warrants, seizures, or subpoenas the contractor receives from another Federal, State, or local agency) for access to Government data, Government-related data, or any associated metadata. The clause also notifies contractors that they must also comply with applicable clauses, regulations, and laws regarding unauthorized disclosure.

Cryptographic Key Services. When providing cryptographic key services under the contract, paragraph (j) of the clause 52.239-YY requires contractors to provide the agency with applicable key material and services; however, the Government reserves the right to implement and operate its own cryptographic key services under the contract.

Operational Technology Equipment List. Paragraph (k) of the clause 52.239-YY requires contractors to develop and maintain a list of the physical location of all operational technology equipment included within the boundary for the non-cloud FIS and provide a copy to the Government, upon request. While the proposed rule does not specify a format for the operational technology equipment list, contractors must ensure that the list includes enough information about the equipment to positively locate and track any movement

of the equipment during contract performance, including details on password protection and the ability for remote access to the equipment.

Binding Operational Directives and Emergency Directives. Paragraph (l) of clause 52.239-YY advises that contractors must comply with Binding Operational Directives (BODs) and Emergency Directives (EDs) issued by CISA that have specific applicability to a FIS used or operated by a contractor. A list of BODs and EDs can be found at *https://www.cisa.gov/directives*. Occasionally, a BOD or ED with an explicit applicability to a FIS used or operated by a contractor will not need to apply to a contract. In such situations, the contracting officer will identify, in paragraph (l)(2) of the clause, any such BODs or EDs that are not applicable to the contract.

Indemnification. Paragraph (m) of the clause 52.239-YY indemnifies the Government from any liability that arises out of the performance of the contract and is incurred because of the contractor's introduction of certain information or matter into Government data or the contractor's unauthorized disclosure of certain information or material. The paragraph serves as a waiver of defense to change the analysis from negligence, which is the defense, to strict liability, which doesn't allow for a defense. The paragraph also provides terms and requirements in the event of a claim or suit against the

Government for such an unauthorized disclosure or introduction of data or information. The proposed text was taken from industry terms of service agreements for cloud services providers.

Subcontracts. Paragraph (n) of the clause 52.239-YY advises contractors that the substance of the clause must be included in any subcontracts issued under the contract that are for services to develop, implement, operate, or maintain a FIS using non-cloud computing services.

Prohibition on IoT Devices. The rule also implements a portion of the "Internet of Things Cybersecurity Improvement Act of 2020" (Pub. L. 116-207), which prohibits agencies from procuring or obtaining, renewing a contract to procure or obtain, or using an IoT device if the agency's Chief Information Officer determines in certain situations that the use of such a device prevents compliance with NIST SP 800-213. The rule advises contracting officers at 39.X03-1(b) of the prohibition and how the prohibition may be waived by the head of the agency if certain criteria are met.

B. FIS using cloud computing services

When acquiring services to develop, implement, operate, or maintain a FIS using cloud computing services, agencies will identify the FIPS Publication 199 impact level and the corresponding Federal Risk and Authorization

Management Program (FedRAMP) authorization level for all applicable cloud computing services in the contract.

Safeguards, controls, and maintenance of certain systems within the United States. Paragraph (c) of the clause 52.239-XX requires contractors to implement and maintain the security and privacy safeguards and controls in accordance with the FedRAMP level specified by the agency, engage in continuous monitoring activities, and provide continuous monitoring deliverables as required for FedRAMP approved capabilities. More information on these deliverables can be found in the "FedRAMP Continuous Monitoring Strategy Guide" at *https://www.fedramp.gov/assets/resources/documents/CSP_Continuous_Monitoring_Strategy_Guide.pdf*.

Additionally, paragraph (c) specifies that, when a system is categorized as having FIPS Publication 199 high impact, contractors must maintain within the United States or its outlying areas (see FAR 2.101) all Government data that is not physically located on U.S. Government premises, unless otherwise specified in the contract.

Government data. Paragraph (f) of the clause 52.239-XX requires contractors to provide and dispose of Government data and Government-related data in the manner and format specified in the contract. Contractors must also provide confirmation to the contracting officer that

such data has been disposed of in accordance with contract closeout procedures.

Other protections. Similar to the requirements for non-cloud FISs in clause 52.239-YY, the clause 52.239-XX: (1) at paragraph (c), reserves the Government's right to implement and operate its own cryptographic key services under the contract; (2) at paragraph (d), specifies the limitations on contractor access to, use, and disclosure of Government data and Government-related data under the contract; (3) at paragraph (e), requires contractors to handle security incident and cyber threat reporting in accordance with proposed FAR clause 52.239-ZZ; (4) at paragraph (f), specifies the terms for the Government's authorized representatives' access to Government and Government-related data, contractor personnel, and contractor facilities; (5) at paragraph (g), requires contractors to notify the contracting officer of any requests from a third-party (including another Federal, State, or local agency) for access to Government data and Government-related data; (6) at paragraph (h), requires contractors to indemnify the Government from any liability that arises out of the performance of the contract because of the contractor's introduction of certain information or matter into Government data or the contractor's unauthorized disclosure of certain information or material;

and (7) at paragraph (i), specifies when to include the substance of the clause in subcontracts.

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 applies section 7 of the Internet of Things Cybersecurity Improvement Act of 2020 (15 U.S.C. 278g-3e) to acquisitions valued at or below the SAT because of the "notwithstanding section 1905" in 15 U.S.C. 278g-3e(a)(2) which applies the Act to such acquisitions. This rule also applies to acquisitions for commercial products, including COTS items, and commercial services because Government data and systems require protection regardless of dollar value or commerciality of the product or service.

To implement paragraphs (a) and (b)(1) of section 7 of the Act, this rule adds a new policy at FAR 39.X02-1(b), Prohibited IoT devices in Federal information systems. The policy prescribed at FAR 39.X02-1(b) applies when agencies are acquiring IoT devices.

A. Applicability to Contracts at or Below the Simplified Acquisition Threshold

41 U.S.C. 1905 governs the applicability of laws to acquisitions at or below the SAT. Section 1905 generally limits the applicability of new laws when agencies are making acquisitions at or below the SAT, but provides that

such acquisitions will not be exempt from a provision of law under certain circumstances, including when the FAR Council makes a written determination and finding that it would not be in the best interest of the Federal Government to exempt contracts and subcontracts in amounts not greater than the SAT from the provision of law. At the time of the final rule the FAR Council does not intend to make a determination to apply 15 U.S.C. 278g-3e to acquisitions at or below the SAT because paragraph (a)(2) of 15 U.S.C. 278g-3e expressly states that it applies to acquisitions in amounts not greater than the SAT; therefore, no additional determination is necessary under 41 U.S.C. 1905.

B. Applicability to Contracts for the Acquisition of Commercial Products and Commercial Services, Including Commercially Available Off-The-Shelf (COTS) Items

41 U.S.C. 1906 governs the applicability of laws to contracts for the acquisition of commercial products and commercial services, and is intended to limit the applicability of laws to contracts for the acquisition of commercial products and commercial services. Section 1906 provides that if the FAR Council makes a written determination that it is not in the best interest of the Federal Government to exempt commercial item contracts, the provision of law will apply to contracts for the acquisition of commercial products and commercial services.

41 U.S.C. 1907 states that acquisitions of COTS items will be exempt from certain provisions of law unless the Administrator for Federal Procurement Policy makes a written determination and finds that it would not be in the best interest of the Federal Government to exempt contracts for the procurement of COTS items.

At the time of the final rule the FAR Council intends to make a determination to apply 15 U.S.C. 278g-3e to acquisitions for commercial products and commercial services. At the time of the final rule, the Administrator for Federal Procurement Policy intends to make a determination to apply 15 U.S.C. 278g–3e to acquisitions for COTS items.

C. Determination(s)

This rule applies to acquisitions for commercial products, including COTS items, and commercial services, because Government data and systems require protection regardless of dollar value or commerciality of the product or service.

IV. Expected Impact of the Rule

The Government anticipates that this rule will reduce administrative costs for contractors interested in providing services to develop, implement, operate, or maintain a FIS. Over time, the FAR Council anticipates this proposed rule, once finalized, will increase competition by

establishing a common set of policies and procedures that apply to FISs.

Establishing uniform requirements for the Government and contractors regarding FISs will significantly assist the Government in protecting Federal information and systems from malicious cyber campaigns that threaten the public and private sectors' security and privacy. Currently, contract requirements for the cybersecurity standards of unclassified FISs are largely based on agency-specific policies and regulations, which can lead to inconsistent security requirements across contracts and unclear, inconsistent, or overly restrictive guidance to contractors. This rule will provide a more consistent and streamlined implementation of cybersecurity standards across the Federal Government.

A. Affected Entities.

This rule proposes two new contract clauses for use when acquiring services to develop, implement, operate, or maintain a FIS. Specifically, the contracting officer will include—

- The clause at FAR 52.239-YY, Federal Information Systems Using Non-Cloud Computing Services, in solicitations and contracts that use or may use non-cloud computing services in performance of the contract; and
- The clause at FAR 52.239-XX, Federal Information Systems Using Cloud Computing Services, in solicitations and

contracts that use or may use cloud computing services in performance of the contract.

According to subject matter experts, there are approximately 140 non-cloud FISs currently being operated or maintained by contractors on behalf of the Government. For this estimate, the Government conservatively assumes that the services for each of these non-cloud FISs are awarded on individual contracts and that each contract is awarded to a unique entity. It is assumed that each of these contracts have a five-year period of performance, and that the Government evenly awards the estimated 140 contracts over a five-year period (20 percent each year). Therefore, the Government estimates it awards 28 contracts ((20 percent * 140 non-cloud FISs) * 1 contract/FIS) to 28 unique contractors (28 contracts = 28 unique entities) annually for the development, implementation, operation, or maintenance of a non-cloud FIS on behalf of the Government.

According to FedRAMP data and subject matter experts, there are approximately 280 unique FedRAMP-authorized and ready cloud service offerings available to the Federal Government. For this estimate, the Government will award approximately 280 contracts for cloud services impacted by this rule over a five-year period (20 percent each year). Based on the number of FedRAMP-authorized offerings, the Government estimates that there are approximately 56 new or revised FIS offerings (20 percent * 280 cloud service

offerings) each year for which the Government contracts. For this estimate, the Government assumes: the number of new or revised FIS offerings the Government contracts for each year is equivalent to the number new FIS impacted by this rule annually; one service provider is responsible for executing all the requirements of this rule for a FIS; and that each FIS is being serviced by a different contractor. Therefore, the Government estimates that 56 unique entities will be awarded a contract annually for the development, implementation, operation, or maintenance of a cloud FIS on behalf of the Government.

Based on the input of subject matter experts, the Government further estimates that:

- Of the 28 contractors that will be awarded a contract each year to operate or maintain a non-cloud FIS, approximately three (10 percent) are small businesses and 25 (90 percent) are other than small businesses.
- Of the 56 contractors that will be awarded a contract each year to operate or maintain a cloud FIS, approximately three (five percent) are small businesses and 53 (95 percent) are other than small businesses.

B. Contractor Compliance Requirements and Estimate of Cost.

The total estimated annualized public costs associated with this FAR rule over a ten-year period (calculated at a 7-percent discount rate) are approximately $55 million

annually, or $388 million in net present value, based on the discussion in paragraphs IV.B.1. through IV.B.7 below.

The following compliance requirements in FAR clause 52.239-YY and 52.239-XX are considered new to the FAR for all Federal contractors that develop, implement, operate, or maintain a FIS using cloud or non-cloud computing services, as applicable:

1. Regulatory Familiarization.

The new FAR clauses are prescribed for use in solicitations and contracts for services to develop, implement, operate, or maintain a FIS. It is expected that all 84 contractors (28 non-cloud FIS contractors + 56 cloud FIS contractors) awarded a contract annually for these services will need, to some degree, to become familiar with the various compliance requirements of the FAR, as well as the requisite and applicable NIST SP guidelines, FIPS Publication standards, CISA BODs and EDs, and FedRAMP requirements, to be prepared to implement and maintain the cybersecurity standards and requirements for a FIS in performance of a Federal contract. It is assumed that most contractors will be familiar with, to some degree, some or all these documents.

Offerors will also need to be familiar with these requirements before submitting a proposal to provide such services. For each of the 84 contractors that receive a contract annually for these services, the Government

estimates that, on average, two other offerors, or a total of 168 offerors (84 contractor awards * 2 unsuccessful offerors) will familiarize themselves with the clause requirements, submit a proposal, but will not receive a contract award.

As a result, it is expected that all 252 (84 contractors + 168 offerors) of these contractors and offerors will be required to become familiar with the various compliance requirements of the rule.

It is estimated that it will take each offeror or contractor eight hours, on average, to review the rule and gain a basic understanding these new requirements. The average wage rate of a contractor employee is estimated to be $57.28 per hour, which is the average of the mean wages reported by the Bureau of Labor Statistics (BLS) for various occupational categories that design, analyze, maintain, and oversee information systems for an organization. A factor of 42 percent, based on the BLS Employer Costs for Employee Compensation Summary dated March 17, 2023 (*https://www.bls.gov/news.release/ecec.nr0.htm*), is applied to the average wage rate to account for total employee benefits paid for by the employer ($57.28 * 1.42 = $81.34), and a factor of 12 percent is then applied to the rate of $81.34 to account for employer overhead, which results in a loaded rate of $91.10 ($81.34 * 1.12) for FIS occupations.

Therefore, the estimated cost for 252 contractors and offerors to familiarize themselves with the rule in year one is approximately $183,700 (252 contractors and offerors * 8 hours/entity * $91.10/hour). The cost accounts for the time needed to comprehend the text of the rule, as well as locate and generally review the requirements within each of the cited documents in the rule.

2. Compliance with NIST Guidelines. All 28 contractors that develop, implement, operate, or maintain a FIS using non-cloud computing services are required by paragraphs (e) and (f) of the new clause 52.239-YY to use or apply various NIST SP guidelines for managing risk, security, and privacy, as applicable. The extent to which each of these guidance documents needs to be implemented by a contractor depends on many variables, including: the extent to which the guidance is already implemented in the contractor's existing practices; the scope and requirements of each contract; the knowledge and expertise of the contractor's employees; the manner in which a contractor chooses to implement a requirement; and the resources and tools available to the contractor in performing the contract.

Based on the discussion in paragraphs IV.B.2.i. through IV.B.2.x. below, the total annual estimated cost for 28 contractors, as applicable, awarded a contract to develop, implement, operate, or maintain an existing or

custom-build, non-cloud FIS on behalf of the Government, to comply with NIST guidelines in year one is approximately $19.6 million, and approximately $12 million each subsequent year for annual maintenance to remain compliant with existing NIST guidelines.

The cost for complying with NIST guidelines accounts for the time it takes contractors to closely read through the documents, analyze the requirements against the current state and identify any necessary changes, and implement and document the change, as needed.

i. NIST SP 800-53. The effort and resources a contractor will expend to comply with NIST SP 800-53 will also vary depending on whether the affected FIS is an existing system or a system that will be custom built to Government specifications.

Existing systems already implement some of the guidelines required by the clause or their implementation has been accepted by the Government, while custom-built systems have no pre-existing controls in place and will require a greater amount of effort and resources to be compliant with the clause. The Government estimates that of the 28 contractors annually awarded a contract to develop, implement, operate, or maintain a non-cloud FIS, approximately six contractors (20 percent) are awarded a contract involving a custom-build system, while the

remaining 22 contractors (80 percent) are awarded a contract involving an existing system.

Contractors awarded a contract involving an existing non-cloud FIS are anticipated to expend between 2,300 and 6,500 hours and $218,000 and $683,000 in labor and materials in year one to implement, and between $127,000 and $478,000 each following year to maintain compliance with NIST SP 800-53. The cost and effort to implement and maintain compliance will vary by contractor depending on various factors, including: the complexity of the information system; the availability of employees with the requisite knowledge and skills to implement the necessary controls; the need to install hardware or software, and the chosen solution, as well as the number of users impacted, the types of devices used, and the complexity of the contractor's network.

Contractors awarded a contract involving a custom build non-cloud FIS will expend between 3,000 and 7,300 hours and between $308,000 and $976,000 in labor and materials in year one to implement, and between $126,000 and $478,000 each following year to maintain compliance with NIST SP 800-53. The cost and effort to maintain compliance will vary by contractor based on the factors discussed above.

ii. NIST SP 800-213. This document provides high level guidance that refers readers to other NIST SP

documents addressed in this rule. Contractors may reference this guidance when their contracts involve IoT devices. As such, the Government assumes that a small percentage of the 28 contractors awarded a contract involving a non-cloud FIS, whose contract also involves IoT devices, may refer to this publication for direction to more detailed policy and guidance regarding the devices; However, the Government does not anticipate contractors expending significant effort reading and familiarizing themselves with the publication and considers these costs to be de minimis.

iii. NIST SP 800-39. NIST SP 800-39 identifies the Government's risk management responsibilities related to information systems. All contractors awarded a contract involving a non-cloud FIS will need to be aware of the requirements of the publication to adequately support the non-cloud FIS on behalf of the Government. As such, the Government assumes all 28 contractors awarded a contract involving a non-cloud FIS will expend effort to read and become more familiar with the publication. It is estimated that a contractor will expend approximately 4 hours reading NIST SP 800-39 in year one to become more familiar with its contents. Using an average loaded wage rate of $91.10 for FIS occupations, the total estimated labor cost for a contractor to comply with NIST SP 800-39 is approximately $370(4 hours * $91.10).

iv. NIST SP 800-37. Contractors will reference this guidance to develop a high-level process to manage system risk through preparation, categorization, control selection, control implementation and assessment, system authorizations, and continuous monitoring. This guidance applies to contracts involving a custom-build system. As such, the Government assumes all 6 contractors awarded a contract involving a custom-build, non-cloud FIS will expend effort to comply with this guidance.

It is estimated that, in year one, a contractor will expend approximately 8 hours reading and ensuring the processes they develop incorporate the high-level guidance of NIST SP 800-37. Using an average loaded wage rate of $91.10 for FIS occupations, the total estimated labor cost for a contractor to comply with NIST SP 800-37 is approximately $730 (8 hours * $91.10).

v. NIST SP 800-207. Contractors will reference this guidance when designing a zero-trust architecture approach for a system. This guidance applies to contracts involving a custom-build system; However, this document is very high level and applies to custom-build requirements in limited circumstances. For these reasons, the Government does not anticipate most contractors needing to read and familiarize themselves with the publication, as its application is unlikely in most custom-build contracts and,

in such circumstances, any time spent reviewing the guidance will be very minimal.

vi. NIST SP 800-160, Volume 1. This guidance applies to contracts involving a custom-build system. Contractors will reference the current version of this guidance for considerations, concepts, tasks, and activities to be taken when designing a system. As such, the Government assumes all 6 contractors awarded a contract involving a custom-build, non-cloud FIS will expend effort to read and familiarize themselves with the publication and make any requisite adjustments to their security design process to be compliant with the guidance.

It is estimated that a contractor will expend approximately 40 hours reading to become more familiar and adjusting the FIS design process to comply with NIST SP 800-160 Volume 1 in year one. Using an average loaded wage rate of $91.10 for FIS occupations, the total estimated labor cost for a contractor to comply with NIST SP 800-160 Volume 1 is approximately $3,600 (40 hours * $91.10).

vii. NIST SP 800-160, Volume 2. When requested by the Government, contractors will reference the current version of this guidance to select, adapt, and use cyber resiliency constructs for new systems, system upgrades, or repurposed systems. This guidance applies to contracts involving a custom-build system. As such, the Government assumes all 6 contractors awarded a contract involving a

custom-build, non-cloud FIS will expend effort to read and become more familiar with the publication.

It is estimated that a contractor will expend approximately 16 hours reading NIST SP 800-160 Volume 2 to become more familiar with its requirements in year one. Using an average loaded wage rate of $91.10 for FIS occupations, the total estimated labor cost for a contractor to comply with NIST SP 800-160 Volume 2 is $1,500(16 hours * $91.10).

viii. NIST SP 800-30. Contractors will reference the current version of this guidance to develop and ensure existing processes prepare for, conduct, communicate results from, and maintain risk assessments over time. This guidance is applicable to all contracts involving a custom-build system, as these processes will need to be developed for those FIS, as well as some contracts involving existing systems where current processes need to be modified to comply with the guidance. As such, the Government assumes all 6 contractors awarded a contract involving a custom-build, non-cloud FIS, and 4 (20 percent * 22) contractors awarded a contract involving an existing, non-cloud FIS will expend effort to read and better familiarize themselves with the publication and develop new or adapt existing processes to the guidance of NIST SP 800-30.

Some contractors awarded a contract involving a non-cloud FIS will reference NIST SP 800-30 to develop and ensure risk assessment processes and procedures for the system incorporate the requirements of the publication. It is estimated that all 6 contractors awarded a contract involving a non-cloud, custom-build FIS, as well as 4 contractors (20 percent) awarded a contract involving an existing non-cloud FIS will expend approximately 120 hours (3 employees * 8 hours/day * 5 days) reading to become more familiar with and developing or adjusting processes and procedures to comply with NIST SP 800-30 in year one. Using an average loaded wage rate of $91.10 for FIS occupations, the total estimated labor cost for a contractor to comply with NIST SP 800-30 is approximately $10,900 (120 hours * $91.10).

ix. NIST SP 800-63-3. Contractors may reference the current version of this guidance for more specific information regarding NIST SP 800-53 controls. As such, the Government assumes that the 28 contractors awarded a contract involving a non-cloud FIS will read and better familiarize themselves with this publication in conjunction with and as a part of their familiarization efforts and costs for NIST SP 800-53.

x. NIST SP 800-34. Contractors will reference the current version of this guidance to align its contingency plans for all IT systems to the requirements of NIST SP

800-34. This guidance will be applicable to all contracts involving a custom-build system, as these plans will need to be developed for when a new non-cloud FIS is being designed, as well as some contracts involving existing systems where current plans need to be modified to comply with the guidance. As such, the Government assumes all 6 contractors awarded a contract involving a custom-build, non-cloud FIS and 4 (20 percent * 22) of the contractors awarded a contract involving an existing, non-cloud FIS will expend effort to read and better familiarize themselves with the publication and develop new or adapt existing plans to the guidance of NIST SP 800-34.

Some contractors awarded a contract involving a non-cloud FIS will reference this guidance when developing new contingency plans for custom-build FISs and reviewing plans for some existing FISs to ensure the contractor's IT systems meet the requirements set forth in NIST SP 800-34. It is estimated that all 6 contractors awarded a contract involving a non-cloud, custom-build FIS, as well as 4 (20 percent) contractors awarded a contract involving an existing non-cloud FIS will expend approximately 120 hours (3 employees * 8 hours/day * 5 days) reading to become more familiar with and developing or adjusting plans to comply with NIST SP 800-34 in year one. Using an average loaded wage rate of $91.10 for FIS occupations, the total

estimated labor cost for a contractor to comply with NIST SP 800-34 is $10,900(120 hours * $91.10).

3. Annual Assessments of the FIS.

Paragraph (d) of the new clause 52.239-YY requires a contractor that develops, implements, operates, or maintains a FIS using non-cloud computing services and that FIS is designated as a moderate or high FIPS Publication 199 impact, to perform an annual, independent assessment of the security of each FIS, which includes an architectural review and penetration testing of the FIS. The contractor must also conduct, at least annually, cyber threat hunting and vulnerability assessment to search for cybersecurity risks, vulnerabilities, and indicators of compromise. Contractors are required to provide the contracting officer with the results of both assessments, including any recommended improvements or risk mitigations identified for the FIS. If the Government chooses not to require the contractor to implement a recommended improvement or risk mitigation and provides the contractor with a rationale for not implementing the recommendation, the contractor is required to document the Government's rationale for not implementing the recommendation in the contractor's system security plan.

Of the 140 non-cloud FISs currently being operated or maintained by contractors on behalf of the Government, the Government estimates that approximately 95 percent of those

systems are designated as moderate or high FIPS 199 impacts. Applying that percentage to the estimated number of contractors annually awarded a contract to develop, implement, operate, or maintain a non-cloud FIS, it is estimated that 27 contractors (95 percent * 28 contractors) will be subject to the annual assessment requirements. Based on the discussion in paragraphs IV.B.3.i. through IV.B.3.iii. below, the total annual estimated cost for 27 contractors that operate or maintain a non-cloud FIS designated as a moderate or high FIPS 199 impact to comply with the annual assessment requirements of the rule is approximately $6.6 million (27 contractors * ($112,000 + $132,000 + $182)). The cost of the annual assessments accounts for the time it takes contractors to prepare for, conduct, document, review, and submit an assessment.

i. Annual Independent Architectural Review and Penetration Test. This annual assessment includes an architectural review of the FIS, as well as penetration testing of the system. Based on the input of subject matter experts, the Government estimates the annual cost for a contractor to obtain an independent security assessment and architectural review of a FIS is approximately $52,000.

The Government estimates that four senior level employees will expend a total of 320 hours (4 individuals * 8 hours * 10 days) to complete the penetration testing of a

FIS. According to subject matter experts, the average loaded wage rate of for a penetration tester is $250.00. The Government estimates the annual cost for a contractor to obtain independent penetration testing of a FIS is $80,000 (320 hours * $250).

Together, the annual cost to a contractor to obtain an independent assessment of the security of a FIS is approximately $132,000 ($52,000 + 80,000).

ii. Cyber Threat Hunting and Vulnerability Assessment. The Government estimates that four senior level employees will expend a total of 448 hours (4 individuals * 8 hours * 14 days) to complete cyber threat hunting and the vulnerability assessment of a FIS. Using an average loaded wage rate of $250.00 for a cyber threat hunter/vulnerability assessor, the Government estimates the annual cost for a contractor to conduct a cyber threat hunting and vulnerability assessment of a FIS is approximately $112,000 (448 hours * $250).

iii. Submission of Assessments. The Government estimates a contractor will spend one hour preparing and submitting each assessment to the Government. Using an average loaded wage rate of $91.10 for FIS occupations, the total annual estimated cost for a contractor that operates or maintains a non-cloud FIS designated as a moderate or high FIPS 199 impact to submit both assessments to the

Government is approximately $182 (1 hour * 2 responses * $91.10).

4. Submission of a Continuous Monitoring Strategy.

Paragraph (f)(7) of the new clause 52.239-YY requires a contractor that develops, implements, operates, or maintains a non-cloud FIS to provide the Government with a continuous monitoring strategy for the FIS (as developed under NIST SP 800-53) that demonstrates an ongoing awareness of information security, vulnerabilities, and threats in order to support risk management decisions, and applies the use of automation, wherever possible; protects vulnerability scan data, logs, and telemetry; and applies the guidance of NIST SP 800-137, "Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations."

All 28 contractors awarded a contract involving a non-cloud FIS will be required to develop or update their continuous monitoring strategy to meet the requirements of this rule. Many contractors will have developed a continuous monitoring strategy to comply with the guidance in NIST 800-53; however, those plans may need to be revised to demonstrate a continuous monitoring strategy. The Government estimates a contractor will spend, on average, 160 hours developing and/or documenting a continuous monitoring strategy, revising their existing strategy, as needed, and submitting the strategy to the Government.

Using an average loaded wage rate of $91.10 for FIS occupations, the total annual estimated cost for a contractor that operates or maintains a non-cloud FIS to submit a continuous monitoring strategy to the Government is approximately $14,600 (160 hours * $91.10).

Based on the information above, the total annual estimated cost for 28 contractors that design, develop, operate, or maintain a non-cloud FIS to comply with the requirement for a continuous monitoring strategy in year one is approximately $408,000 (28 contractors * 160 hours * $91.10). The cost of the continuous monitoring strategy accounts for the time needed to analyze, develop, and document a strategy or review an existing strategy and make revisions, and prepare and submit the strategy to the Government.

5. Develop and Maintain a List of Operational Technology Equipment.

Paragraph (k) of the new clause 52.239-YY requires all contractors that develop, implement, operate, or maintain a FIS using non-cloud computing services to develop and maintain a list of the physical location and other pertinent data on all of the operational technology (OT) equipment included within the boundary of the FIS. Contractors must provide the Government with a copy of the current and/or historical lists, upon request. All 28 contractors awarded a contract involving a non-cloud FIS

will be required to develop, submit, and maintain a list of OT equipment.

The Government estimates that a contractor will expend approximately 80 hours developing the list in year one, and 40 hours updating and maintaining the list each year thereafter. Using an average loaded wage rate of $91.10 for FIS occupations, the annual estimated cost for a contractor that operates or maintains a non-cloud FIS to develop a list of OT equipment is approximately $7,300 (80 hours * $91.10), and approximately $3,600 to maintain the list thereafter.

It is estimated that the Government will annually request 6 (20 percent * 28 contractors) contractors provide a copy of the OT equipment list to the Government. It is estimated that a contractor will spend one hour preparing and submitting the list to the Government. Using an average loaded wage rate of $91.10 for FIS occupations, the total annual estimated cost for contractors to submit the OT equipment lists to the Government is approximately $550 (6 contractors * 1 hours * $91.10).

Based on the discussion above, the total annual estimated cost for 28 contractors that develop, implement, operate, or maintain a non-cloud FIS to develop the required OT equipment list in year one is approximately $204,000 (28 contractors * 80 hours * $91.10), and approximately $102,000 (28 contractors * 40 hours * $91.10)

each following year to maintain the list annually. The cost accounts for the time needed to identify the requisite equipment, gather the required data, and document or update the information.

6. Binding Operational Directives and Emergency Directives.

Paragraph (l) of the new clause 52.239-YY requires all contractors that develop, implement, operate, or maintain a FIS using non-cloud computing services to comply with any BODs or EDs issued by CISA that have a specific applicability to a FIS used or operated by a contractor. All 28 contractors awarded a contract involving a non-cloud FIS will be required to comply with CISA BODs and EDs. Currently, there are approximately 15 BODs and 10 EDs posted on CISA's cybersecurity directives website. The Government anticipates that contractors have already implemented all or some of the requirements of all or some BODs or EDs, as part of their company's cybersecurity health. As a result, the Government estimates that the requirements of approximately half of the BODs, or 8 BODS, and EDs, or 5 EDs, will still need to be implemented by a contractor because of this rule in year one. The Government estimates that approximately 3 new BODs or EDs will be issued, and need to be implemented by contractors, in each following year.

The requirements of the BODs and EDs vary in depth, scope, and complexity depending on the topic and issue being addressed. For this reason, subject matter experts estimate that, on average, it costs a contractor $10,000 to implement a new BOD or ED. As a result, the total annual estimated cost for a contractor that operates or maintains a non-cloud FIS to implement existing CISA BODs and EDs in year one is approximately $130,000 (13 x $10,000), and approximately $30,000 to implement new BODs or EDs issued each following year.

Based on the discussion above, the total annual estimated cost for 28 contractors that develop, implement, operate, or maintain a non-cloud FIS to implement the requirements of CISA BODs and EDs in year one is approximately $3,640,000 (28 contractors * 13 BODs and EDs * $10,000), and approximately $840,000 (28 contractors * 3 BODs & EDs * $10,000) each following year to maintain the list annually. The cost accounts for the time needed to identify and implement the requisite requirements, as well as any material cost.

7. FedRAMP Cloud Computing Security and Privacy Requirements.

The new clause 52.239-XX requires contractors that develop, implement, operate, or maintain a FIS using cloud computing services to implement and maintain security and privacy safeguards and controls for the system in

accordance with the FedRAMP level specified in the contract, as well as certain requirements on multifactor authentication, administrative accounts, and consent banners specified in the contract. All 56 contractors awarded a contract to develop, implement, operate, or maintain a cloud FIS on behalf of the Government will expend effort and resources to be compliant with cloud computing security requirements at the FedRAMP level specified in the contract and certain requirements specified in the contract.

FedRAMP safeguards and controls are based upon the requirements of NIST SP 800-53 and specify the requirements that must be met for a cloud offering depending on the designation of the information system as a low, moderate, or high FIPS 199 impact level, which then equates to a single FedRAMP impact level. Based on a survey of the FedRAMP Marketplace website, most of the FedRAMP-authorized cloud service providers offer solutions designated as moderate FedRAMP impact level; Therefore, the Government bases the effort and resources needed to implement the requirements of FAR clause 52.239-XX on a cloud FIS designated as a FedRAMP moderate impact level.

The safeguards and controls required to meet a FedRAMP moderate impact level include and build upon the NIST SP 800-53 requirements for existing non-cloud FIS systems. As such, the rule uses the costs to implement NIST SP 800-53

for non-cloud FIS as a starting point and then accounts for the additional costs and impacts for contractors to implement approximately 16 additional NIST SP 800-53 controls, which are not required for non-cloud FISs, to be compliant with FedRAMP moderate impact level requirements. Subject matter expects estimate that the effort to implement these 16 additional controls, and those requirements for multifactor authentication, administrative accounts, and consent banners, is approximately 25 percent of the total estimated hours and cost to implement NIST SP 800-53.

Therefore, contractors awarded a contract involving a cloud FIS are anticipated to expend between 2,900 (2,300 hours * 1.25) and 8,200 hours (6,500 hours * 1.25) and $273,000 ($218,000 * 1.25) and $854,000 ($683,000 * 1.25) in labor and materials in year one to implement, and between $158,000 ($127,000 * 1.25) and $598,000 (478,000 * 1.25) each following year to maintain compliance with NIST SP 800-53 and the contract requirements on multifactor authentication, administrative accounts, and consent banners.

Based on the discussion above, the total annual estimated cost for 56 contractors that develop, implement, operate, or maintain a cloud FIS to maintain compliance with FedRAMP requirements, and the requirements specified in the contract as identified above, in year one is

approximately $46 million, and approximately $32,000,000, each following year to maintain compliance with FedRAMP requirements and the contract, as specified. The cost of the compliance includes the time needed to read and implement NIST SP 800-53 requirements, as well as the additional NIST SP 800-53 controls needed to be compliant with FedRAMP and the contract requirements regarding multifactor authentication, administrative accounts, and consent banners.

The following is a summary of the total initial and subsequent year costs to the public as described in section IV.

Requirement	# of Entities Impacted	Estimated Total Cost - First Year	Estimated Total Cost - Each Subsequent Year
Regulatory Familiarization	252	$183,700	N/A
Compliance with NIST Guidelines	28	$19,600,000	$12,000,000
Annual Assessments	27	$6,600,000	$6,600,000
Continuous Monitoring Strategy	28	$408,000	N/A
Develop and Maintain OT List	28	$204,000	$102,000
Binding Operational Directives and Emergency Directives	28	$3,640,000	$840,000
FEDRamp Compliance	53	$46,000,000	$32,000,000
	TOTALS	$76,635,700	$51,543,000

C. Government Compliance Requirements.

The total estimated annualized costs to the Government associated with this FAR rule over a ten-year period are approximately $136,000 (calculated at a 7-percent discount rate).

The following specific compliance requirements related to FAR clause 52.239-XX and 52.239-YY are tasks for the Government:

1. Review and Analyze Annual Assessments.

The Government must review and analyze each of the 54 assessments provided by contractors annually (see 39.X03(c)) and provide a recommendation to the contractor to implement, or a rationale for not implementing, each recommendation in the contractor's assessments.

It is estimated that a General Schedule (GS) 15/step 5 employee will spend 20 hours reviewing, analyzing, and drafting recommendation responses for each assessment. The wage rate of a GS 15/step 5 employee is $74.35 per hour, according to the Office of Personnel Management (OPM) 2023 GS Locality Pay Table for the rest of the United States (*https://www.opm.gov/policy-data-oversight/pay-leave/salaries-wages/salary-tables/pdf/2023/RUS_h.pdf*). A factor of 36.25 percent, based on OMB M-08-13, Update to Civilian Position Full Fringe Benefit Cost Factor, is applied to the average wage rate to account for total employee benefits paid for by the Government ($74.35 * 1.3625 = $101.30), and a factor of 12 percent is then applied to the rate of $101.30 to account for overhead, which results in a loaded rate of $113.46($101.30 * 1.12).

Based on the discussion above, the total annual estimated cost for the Government to review, analyze, and

respond to 54 annual assessment submissions each year is approximately $122,537 (54 responses * 20 hours * $113.46).

2. Review List of Operational Technology Equipment.

Upon submission, the Government must review approximately six lists of OT equipment submitted by contractors each year (see 39.X03(k)).

It is estimated that a GS 15/step 5 employee will spend 20 hours reviewing, analyzing, and processing a contractor's submission. Using an average loaded wage rate of $113.46 for GS Schedule 15/step 5 employees, the total annual estimated cost for the Government to review, analyze, and file six OT equipment list submissions each year is approximately $13,615 (6 responses * 20 hours * $113.46).

3. Review Continuous Monitoring Strategy.

Upon submission, the Government must review approximately 28 continuous monitoring strategies provided by contractors each year (see 39.X03(f)). It is estimated that a GS 15/step 5 employee will spend 20 hours reviewing, analyzing, and processing a contractor's submission. Using an average loaded wage rate of $113.46 for GS 15/step 5 employees, the total annual estimated cost for the Government to review, analyze, and file 28 continuous monitoring strategy submissions each year is approximately $63,538 (28 responses * 20 hours * $113.46).

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 rule is a significant regulatory action under E.O. 12866, and therefore, was subject to review under Section 6(b) of E.O. 12866, Regulatory Planning and Review, dated September 30, 1993.

VI. Regulatory Flexibility Act

DoD, GSA, and NASA do not expect this proposed rule, when finalized, to 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, because the rule applies to a small number of entities that develop, implement, operate, or maintain a FIS on behalf of the Government. However, an Initial Regulatory Flexibility Analysis (IRFA) has been performed and is summarized as follows:

DoD, GSA, and NASA are proposing to amend the Federal Acquisition Regulation (FAR) to implement standardized cybersecurity contractual requirements across Federal agencies for unclassified Federal Information Systems (FIS) pursuant to recommendations received in accordance with paragraph (i) of section 2 of E.O. 14028, "Improving the Nation's Cybersecurity," dated May 12, 2021.

The objective of this rule is to implement standardized cybersecurity requirements in Federal contracts for services to develop, implement, operate, or maintain a FIS on behalf of the Government. This rule will help protect and secure FISs, while streamlining the cybersecurity requirements for applicable contracts and improving contractor and Federal compliance with cybersecurity requirements for these systems. The legal basis for this rule is paragraph (i) of section 2 of Executive Order 14028, "Improving the Nation's Cybersecurity," dated May 12, 2021; and paragraphs (a) and (b)(1) of section 7 of the Internet of Things (IoT) Cybersecurity Improvement Act of 2020 (Pub. L. 116-207). Promulgation of FAR regulations is 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.

This proposed rule will impact small businesses awarded a contract to develop, implement, operate, or maintain a FIS on behalf of the Government. The Government acknowledges that large businesses awarded a contract for such services may further subcontract some of the services that are subject to the requirements of the clauses. As such, the Government estimates that up to an additional seven small business entities may receive a subcontract to develop, implement, operate, or maintain a FIS under a prime contract for the same services.

The responsibilities prescribed to contractors under this rule apply per FIS, not per contractor or subcontractor. Multiple entities will not be responsible for implementing or executing the same requirement for the same FIS; As such, the Government describes the impact of this rule on small business under the assumption that each of the responsibilities described below will be subcontracted to a small business at least once annually.

According to subject matter experts, there are approximately 140 non-cloud FISs currently being operated or maintained by contractors on behalf of the Government. The Government estimates it awards 28 contracts ((20 percent * 140 non-cloud FISs) * 1 contract/FIS) to 28 unique contractors (28 contracts = 28 unique entities) annually for the development, implementation, operation, or maintenance of a non-cloud FIS on behalf of the Government. Of the 28 contractors to be awarded a contract each year to operate or maintain a non-cloud FIS, approximately three (28 contractors * 10 percent) are small businesses.

According to FedRAMP data and subject matter experts, there are approximately 280 unique FedRAMP-authorized and ready cloud service offerings available to the Federal Government. Based on the number of FedRAMP-authorized offerings, the Government estimates that there are approximately 56 new or revised FIS offerings (20 percent * 280 cloud service offerings) each year for which the Government contracts. Therefore, the Government estimates that 56 unique entities to be awarded a contract annually for the development, implementation, operation, or maintenance of a cloud FIS on behalf of the Government, of which approximately three (56 contractors * five percent) are small businesses. The proposed rule requires contractors awarded a contract or subcontract to develop, implement, operate, or maintain a FIS to read and become familiar with the rule, as well as review the applicable standards documents identified in the rule. The proposed rule also requires contractors awarded a contract or subcontract to develop, implement, operate, or maintain a FIS using other than cloud computing services (i.e., "non-cloud FIS") to: (1) Develop and maintain a list of the physical location of all operational technology (OT) equipment included within the boundary of the non-cloud FIS; (2) When requested by the Government, submit a copy of the OT equipment list to the Government; (3) Submit a copy of their continuous monitoring strategy for the FIS; and (4) For FISs categorized as FIPS Publication 199 moderate or high security

impact, submit the results of: an annual independent assessment of the security of the FIS, and an annual cyber threat hunting and vulnerability assessment.

A. Regulatory Familiarization and Standards Document Reviews.

It is estimated that approximately all six small business entities, and up to seven small business subcontractor entities, awarded a contract to design, implement, operate, or maintain a FIS on behalf of the Government will need to become familiar with the various compliance requirements of the new clauses 52.239-YY or 52.239-XX, as well as review any applicable standards documents, to be prepared to develop, implement, operate, or maintain a cloud and/or non-cloud FIS, as applicable.

B. Develop and Submit OT Equipment List.

It is estimated that approximately three small business entities, and up to seven small business subcontractor entities, will be awarded a contract or subcontract annually to develop, implement, operate, or maintain a non-cloud FIS. Each of these entities, will be required to develop, maintain, and submit a list of OT equipment for the duration of the contract. The list must include: (1) the identification and location of any controllers, relays, sensors, pumps, actuators, Open Platform Communications Unified Architecture devices, and other industrial control system devices, as well as all the IP addresses assigned to the different hardware components, used in performance of the contract; (2) An explanation of whether the device is password protected and, if so, whether it can be changed, (3) an explanation of whether the device is accessible remotely; and (4) whether multi-factor authentication is present and enabled. The location information in the list must include enough detail to affirmatively locate the OT equipment, when necessary, and track any movement of such equipment during performance of the contract. It is estimated that one of these three small business entities, and up to seven small business subcontractor entities, will be asked to submit the OT equipment list to the Government each year.
To develop and maintain the list of OT equipment, a small business will need at least one employee within an information system occupation series (e.g., computer system analyst, information security analyst, system administrator, network architect) to identify the requisite devices used in performance of the contract, track the location of such devices as changes occur, and update and modify the OT equipment list as necessary.

C. Submit Continuous Monitoring Strategy.

All three small business entities, and up to seven small business subcontractor entities, awarded a contract annually to develop, implement, operate, or maintain a non-cloud FIS will be required to submit a copy of their continuous monitoring strategy for the FIS that demonstrates an ongoing awareness of information security, vulnerabilities, and threats in order to support risk management decisions, and applies the use of automation, wherever possible; protects vulnerability scan data, logs, and telemetry; and applies the guidance of NIST SP 800-137, " Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations." A small business will need at least one employee within an information system occupation series (e.g., computer system analyst, information security analyst, system administrator, network architect) to review and submit the continuous monitoring strategy.

D. Submit Annual Assessments.

Of the 140 non-cloud FISs currently being operated or maintained by contractors on behalf of the Government, the Government estimates that

approximately 95 percent of those systems are designated as moderate or high FIPS 199 impacts. Applying that percentage to the estimated number of contractors annually awarded a contract to develop, implement, operate, or maintain a non-cloud FIS, it is estimated that 27 contractors (95 percent * 28 contractors), of which 2 are estimated to be small business, will be subject to the annual assessment requirements.

These two small business entities, and up to seven small business subcontractor entities, will be awarded a contract with a FIS designated as moderate or high FIPS Publication 199 impact and be required to submit the results of the two annual assessments to the Government. The assessment of the security of the FIS must be an independent assessment that is not conducted by the contractor. The cyber threat hunting and vulnerability assessment may be completed by the contractor. A small business must submit the results of both assessments, including any recommended improvements or risk mitigations identified for the FIS, to the Government. A small business will need at least one employee within an information system occupation series to review and submit the annual assessments to the Government, as well as implement any recommended solutions resulting from the assessments. If an entity chooses to conduct the cyber threat hunting and vulnerability assessment on their own, the entity will need at least one subject matter expert in cyber threat hunting and vulnerability assessment, as well as experience with system assessment, analysis, and audit.

This rule proposes to standardize common cybersecurity contractual requirements across Federal agencies. To do so, E.O. 14028 required a review of agency-specific cybersecurity requirements that currently exist as a matter of law, policy, or contract to form the recommendation for the standardized contract language proposed in this rule. As a result, this rule may duplicate, overlap, or conflict with existing agency-specific cybersecurity contract clauses. Section 2. Paragraph (k) of the E.O. resolves the issue of duplication, overlap, or conflict by requiring agencies, upon final publication of this rule, to update their agency-specific cybersecurity requirements to remove any requirements that are duplicative of this rule. There are no known significant alternative approaches to the proposed rule.

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 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 2021-019)", 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 Standardizing Cybersecurity Requirements for Unclassified Federal Information Systems to the Office of Management and Budget.

A. Public reporting burden for this collection of information:

1. Submit Annual Assessment of FIS.

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information.

The annual reporting burden estimated as follows:

Respondents/Recordkeepers: 27.

Total Annual Responses: 54.

Total Burden Hours: 54.

This estimate is based on two responses per respondent.

2. Maintain and Submit a List of Operational Technology Equipment.

The public recordkeeping burden for this collection of information is estimated to annually require one recordkeeper who spends 80 hours per contract to maintain the list:

Recordkeepers: 28.

Total annual records: 28.

Total recordkeeping burden hours: 2,240.

The public reporting burden for this collection of information is estimated to average 1 hour per response to review and submit the list. The annual reporting burden is estimated as follows:

Respondents: 6.

Total Annual Responses: 6.

Total Burden Hours: 6.

This estimate is based on one response per respondent.

3. Submit Continuous Monitoring Strategy.

Public reporting burden for this collection of information is estimated to average 160 hours per response to develop, document, review, and submit the strategy. The annual reporting burden is estimated as follows:

Respondents: 28.

Total Annual Responses: 28.

Total Burden Hours: 4,480.

This estimate is based on one response per respondent.

B. Request for Comments Regarding Paperwork Burden. Submit comments on this collection of information no later than [**INSERT DATE 60 DAYS AFTER 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, Standardizing Cybersecurity Requirements for Unclassified Federal Information Systems. 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, Standardizing Cybersecurity Requirements for Unclassified Federal Information Systems, in all correspondence.

List of Subjects in 48 CFR Parts 1, 2, 4, 7, 10, 11, 12, 37, 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, 37, 39, and 52 as set forth below:

1. The authority citation for 48 CFR parts 1, 2, 4, 7, 10, 11, 12, 37, 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, entries for "52.239-XX" and "52.239-YY" and its corresponding OMB control No. "9000-XXXX" to read as follows:

1.106 OMB approval under the Paperwork Reduction Act.

*****

FAR segment	OMB control No.
* * * * * * *	
52.239-XX	9000-XXXX
52.239-YY	9000-XXXX
* * * * * * *	

PART 2-DEFINITIONS OF WORDS AND TERMS

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

a. In the definition of "Component", removing from the end of paragraph (3) the word "and"; removing from the

end of paragraph (4) “52.225-23(a).” and adding “52.225-23(a); and” in its place; and adding a new paragraph (5);

b. Removing the definitions “Federally-controlled information system” and “Information and communication technology (ICT)”;

c. Adding in alphabetical order the definitions “Federal information system”, “Government data”, “Information”, “Information and communications technology (ICT)”, and “Information system”;

d. In the definition of “Information technology”, revising paragraph (3)(ii); and

e. Adding in alphabetical order the definitions “Internet of Things (IoT) devices”, “Operational technology”, “Telecommunications equipment”, and “Telecommunications services”.

The revisions and additions read as follows:

2.101 Definitions.

* * * * *

(b) * * *

(2) * * *

Component * * *

* * * * *

(5) Subpart 39.X, see the definition in 39.X01.

* * * * *

Federal information system—

(1) Means an information system (44 U.S.C. 3502(8)) used or operated by an agency, by a contractor of an agency, or by another organization, on behalf of an agency;

(2) *On behalf of an agency* as used in this definition, means when a contractor uses or operates an information system or maintains or collects information for the purpose of processing, storing, or transmitting Government data, and those activities are not incidental to providing a service or product to the Government (32 CFR part 2002).

* * * * *

Government data means any information, (including metadata), document, media, or machine-readable material regardless of physical form or characteristics that is created or obtained by the Government, or a contractor on behalf of the Government, in the course of official Government business.

* * * * *

Information, as used in subparts 4.19 and 39.X, means any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, electronic, or audiovisual forms (see Office of Management and Budget (OMB) Circular No. A-130, Managing Information as a Strategic Resource).

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.

Information technology * * *

* * * * *

(3) * * *

(ii) Is operational technology.

* * * * *

Internet of Things (IoT) devices means, consistent with section 2 paragraph 4 of Public Law 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

4.1301 [Amended]

4. Amend section 4.1301 by removing from paragraphs (a) and (b) "Federally-controlled information" and adding "Federal information" in their places; respectively.

4.1303 [Amended]

5. Amend section 4.1303 by removing from the text "Federally-controlled information" and adding "Federal information" in its place.

4.1901 [Amended]

6. Amend section 4.1901 by removing the definitions of "Information" and "Information system".

PART 7—ACQUISITION PLANNING

7. Amend section 7.103 by—

a. Removing from paragraph (q) "information and communication technology" and adding "information and communications technology" in its place; and

b. Adding paragraph (z).

The addition reads as follows.

7.103 Agency-head responsibilities.

* * * * *

(z) For service acquisitions that will require a contractor to develop, implement, operate, or maintain a Federal information system, ensuring that acquisition planners (see 2.101(b)), in consultation with the agency's authorizing official (see 39.X01), develop requirements in accordance with the procedures at 39.X02-1 and 39.X02-2.

8. Amend section 7.105 by removing from paragraph (b)(18)(iii) "Federally-controlled information" and adding "Federal information" in its place and adding paragraph (b)(18)(v) to read as follows:

7.105 Contents of written acquisition plans.

* * * * *

(b) * * *

(18) * * *

(v) For service acquisitions that will require a contractor to develop, implement, operate, or maintain a Federal information system, discuss compliance with 39.X02-1 and 39.X02-2.

* * * * *

PART 10—MARKET RESEARCH

10.001 [Amended]

9. 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

11.002 [Amended]

10. Amend section 11.002 by removing from paragraph (f)(1)(i) "information and communication technology" and adding "information and communications technology" in its place.

PART 12—ACQUISITION OF COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES

12.202 [Amended]

11. Amend section 12.202 by removing from paragraph (d) "information and communication technology" and adding "information and communications technology" in its place.

PART 37—SERVICE CONTRACTING

37.000 [Amended]

12. Amend section 37.000 by removing from the text "information technology" and adding "information and communications technology" in its place.

PART 39—ACQUISITION OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

13. Revise the heading for part 39 to read as set forth above.

14. Amend section 39.000 by removing from paragraph (a) "Management of Federal Information Resources" and adding "Managing Information as a Strategic Resource" in its place; and 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)).

15. Amend section 39.001 by revising the first sentence of paragraph (a) and revising 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.

16. Revise subpart 39.2 heading to read as follows:

Subpart 39.2—Information and Communications Technology Accessibility

* * * * *

39.201 [Amended]

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

18. Add a new subpart 39.X to read as follows:

Subpart 39.X Federal Information Systems.

39.X00 Scope of subpart.

This subpart provides policies and procedures for acquiring services to develop, implement, operate, or maintain a Federal information system (FIS) (E.O. 14028, Improving the Nation's Cybersecurity, dated May 12, 2021). This subpart does not apply to National security systems (see 39.002).

39.X01 Definitions.

As used in this subpart–

Administrative account means a user account with full privileges (i.e., with full function and access rights) intended to be used only when performing management tasks, such as installing updates and application software, managing user accounts, and modifying operating system and application settings.

Authorization boundary means all components of an information system to be authorized for operation by an

authorizing official. This excludes separately authorized systems to which the information system is connected (OMB Circular No. A-130).

Authorizing official means a senior Federal official or executive with the authority to authorize (i.e., assume responsibility for) the operation of an information system or the use of a designated set of common controls at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation (OMB Circular No. A-130).

Cloud computing means a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud computing is characterized by on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service; and includes service models such as software-as-a-service, infrastructure-as-a-service, and platform-as-a-service (NIST SP 800-145).

Component means a discrete identifiable information and operational technology asset that represents a building block of a system and may include hardware, software, and firmware.

Cyber supply chain risk means the potential for harm or compromise that arises as a result of cybersecurity risks from suppliers, their supply chains, and their products or services. This includes risks that arise from threats exploiting vulnerabilities or exposures within products and services traversing the supply chain as well as threats or exposures within the supply chain itself. The level of risk depends on the likelihood that relevant threats may exploit applicable vulnerabilities and the consequential potential impacts (NIST SP 800-161 and 800-203).

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 primarily applied to the Government data.

High value asset means Government data or a Federal information system that is designated as a high value asset pursuant to OMB Memorandum M-19-03, Strengthening the

Cybersecurity of Federal Agencies by enhancing the High Value Asset Program.

Media means physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, large-scale integration memory chips, and printouts onto which information is recorded, stored, or printed within an information system (NIST SP 800-37).

Metadata means information describing the characteristics of data including, but not limited to, structural metadata that describes data structures (e.g., data format, syntax, and semantics) and descriptive metadata that describes data contents (e.g., information security labels) (NIST SP 800-53).

Service account means an account used by machines, e.g., an operating system, application, process, or service, not used by a human.

39.X02 Procedures.

All FIS require protection as part of good risk management practices. A contract for services to develop, implement, operate, or maintain a FIS may require contractors to utilize cloud computing services, computing services other than cloud computing services (i.e., non-cloud computing services), or both service approaches in performing the contract. Each service approach requires

certain compliances and standards to be met to ensure appropriate FIS protection.

39.X02-1 Federal information systems using non-cloud computing services.

(a) Contracting officer verification.

(1) *Requirement criteria.* When acquiring services to develop, implement, operate, or maintain a FIS using non-cloud computing services, the contracting officer shall verify with the requiring activity that the requirement—

(i) Categorizes the FIS based on an impact analysis of the information processed, stored, and transmitted by the system (see the current version of Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, for additional information);

(ii) Identifies a set of controls to protect the FIS based on an assessment of risk in accordance with—

(A) The current version of FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems;

(B) The current version of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53B, Control Baselines for Information Systems and Organizations; and

(C) Agency procedures (see paragraph (a)(2) of this section for mandatory controls to be addressed in all requirements);

(iii) Includes the FIPS Publication 199 impact level (paragraph (a)(1)(i) of this section) and the identified controls (paragraph (a)(1)(ii) of this section) in the contract;

(iv) Identifies any Cybersecurity and Infrastructure Security Agency (CISA) Binding Operational Directives and Emergency Directives (from the list at *https://www.cisa.gov/directives*) that will not apply to the requirement (see fill-in at paragraph (l)(2) of 52.239-YY); and

(v) Addresses each of the elements identified at 52.239-YY(f), as applicable.

(2) *Mandatory controls.* The controls identified in paragraph (a)(1)(ii) of this section must address the following requirements:

(i) *Multifactor authentication.*

(A) All accounts other than service accounts must employ multifactor authentication that meets or exceeds Authenticator Assurance Level 2 (AAL2), as defined in the most recent version of NIST SP 800-63B, Digital Identity Guidelines: Authentication and Lifecycle Management. Agencies may mandate accounts for Government or contractor personnel requiring phishing resistant

multifactor authentication exceeding AAL2, depending on the sensitivity of the system or non-public data accessed.

(B) Any administrative access must be conducted using a hardware-based multifactor cryptographic device authenticator.

(ii) *Administrative accounts*.

(A) All systems and services provided shall have unique administrative accounts, with the exception of service accounts.

(B) Any accounts that administer any part of the systems used in the performance of the contract, to include support systems and infrastructure, shall be considered part of the system authorization boundary and must have unique administrative accounts that are unique and exclusive to agency systems. Administrator accounts must be disclosed, upon request by the contracting officer.

(iii) *Consent banners*. Login and consent banners must be deployed on all systems and networks. Such banners must be consistent with CISA guidance at *https://www.cisa.gov/publication/guidance-consent-banners*. The contract may include more specific requirements for consent banners; such requirements will be consistent with the CISA guidance linked above;

(iv) *Internet of Things devices*. Apply any additional cybersecurity requirements necessary for IoT devices located within the boundary of the FIS in

accordance with the current version of NIST SP 800-213, IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements; and

(v) *Annual assessments.* For a FIS designated as a moderate or high FIPS Publication 199 impact, specify the specific requirements for the annual assessments (see FAR 52.239-YY(d)).

(b) *Prohibited IoT devices in Federal information systems.* The Internet of Things Cybersecurity Improvement Act of 2020 (Pub. L. 116-207) prohibits agencies from procuring or obtaining, renewing a contract to procure or obtain, or using an IoT device, if the agency's Chief Information Officer determines (during a review required by 40 U.S.C. 11319(b)(1)(C) of a contract for such device) that the use of such a device prevents compliance with NIST SP 800-213.

(1) The head of the agency may waive the prohibition in this paragraph (b) if the agency's Chief Information Officer determines, in writing, that—

(i) A waiver is necessary in the interest of national security;

(ii) Procuring, obtaining, or using such device is necessary for research purposes; or

(iii) The device is secured using alternative and effective methods appropriate to the function of the device.

(2) When the prohibition is waived in accordance with 39.X02-1(b)(1), contracting officers shall obtain confirmation of the waiver from the agency's Chief Information Officer and document the confirmation in the contract file.

39.X02-2 Federal information systems using cloud computing services.

When acquiring services to develop, implement, operate, or maintain a FIS using cloud computing services, the contracting officer shall verify with the requiring activity that the requirement—

(a) Specifies the FIPS Publication 199 impact level and the Federal Risk and Authorization Management Program (FedRAMP) authorization level that corresponds with the FIPS Publication 199 impact level for all applicable cloud computing services;

(b) For systems categorized as FIPS Publication 199 high impact—

(1) Ensures all Government data is maintained (i.e., stored or processed) within the United States and its outlying areas (see 2.101(b)) or is physically located on U.S. Government premises, unless otherwise authorized in writing by the Authorizing Official for the information system; or

(2) When another location is authorized for the maintenance of Government data in accordance with paragraph

(b)(1), specifies the location(s) authorized by the Authorizing Official for the information system;

(c) Specifies the format(s) in which all Government data and Government-related data is to be received from the contractor;

(d) Specifies how the contractor must dispose of Government data and Government-related data; and

(e) Complies with the following requirements—

(1) *Multifactor authentication*.

(i) All accounts other than service accounts must employ multifactor authentication that meets or exceeds Authenticator Assurance Level 2 (AAL2), as defined in the most recent version of NIST SP 800-63B, Digital Identity Guidelines: Authentication and Lifecycle Management. Agencies may mandate accounts for Government or contractor personnel requiring phishing resistant multifactor authentication exceeding AAL2, depending on the sensitivity of the system or non-public data accessed.

(ii) Any administrative access must be conducted using a hardware-based multifactor cryptographic device authenticator.

(2) *Administrative accounts*.

(i) All systems and services provided shall have unique administrative accounts, with the exception of service accounts.

(ii) Any accounts that administer any part of a system used in the performance of the contract, to include support systems and infrastructure, shall be considered part of the system authorization boundary and must have unique administrative accounts that are unique and exclusive to agency systems. Administrator accounts must be disclosed, upon request by the contracting officer.

(3) *Consent banners*. Login and consent banners must be deployed on all systems and networks. Such banners must be consistent with CISA guidance at *https://www.cisa.gov/publication/guidance-consent-banners*.

The contract may include more specific requirements for consent banners; such requirements will be consistent with the CISA guidance linked above.

39.X03 Contracting officer coordination.

The contracting officer shall coordinate the following requests and submissions with the requiring activity (to enable coordination with the agency chief information security officer, senior agency official for privacy, and agency legal counsel, as necessary)—

(a) Any request for information or access pursuant to the clause at 52.239-ZZ, Incident and Threat Reporting and Incident Response Requirements for Products or Services Containing Information and Communications Technology (ICT);

(b) A submission of a reportable incident pursuant to FAR clause 52.239-ZZ, when such incident involves a FIS;

(c) The contractor's annual, independent assessment of the security of each FIS (52.239-YY(d)(1)(iii)). If received from the requiring activity, the contracting officer shall provide the contractor with the agency's request to implement or rationale for not implementing a recommendation for improvement or mitigation (52.239-YY(d)(1)(iv) and (v));

(d) A contractor's request to use Government-related data for a purpose other than to manage the operational environment that supports the Government data information (52.239-XX(d)(2));

(e) A contractor's submission of its system security plan, when requested by the agency (52.239-YY(e)(3)(ii));

(f) A contractor's submission of its continuous monitoring strategy for the FIS (52.239-YY(f)(7));

(g) A contractor's request to implement alternative, additional, or compensating security controls, to include those pertaining to cyber supply chain risk management, not otherwise identified in the contract (52.239-YY(g));

(h) A contractor's request to use Government metadata for a purpose other than to manage the operational environment that supports the Government data (52.239-YY(i)(2));

(i) A contractor's notification of a third-party request for access to Government data or any associated metadata, or access to information systems with access to

Government data or any associated metadata (52.239-YY(i)(3));

(j) A contractor's request to publish or disclose the details of any safeguards either designed or developed by the contractor under the contract, or otherwise provided by the Government (52.239-YY(i)(4));

(k) A contractor's submission of its operational technology equipment list, when requested by the agency (52.239-YY(k)(3)); and

(l) Any other relevant contractor or third-party requests for access or data not covered herein.

39.X04 Contract clauses.

When acquiring services to develop, implement, operate, or maintain a FIS, the contracting officer shall insert—

(a) The clause at 52.239-YY, Federal Information Systems Using Non-Cloud Computing Services, in solicitations and contracts that use, or are anticipated to use, non-cloud computing services in performance of the contract; and

(b) The clause at 52.239-XX, Federal Information Systems Using Cloud Computing Services, in solicitations and contracts that use, or are anticipated to use, cloud computing services in performance of the contract.

PART 52—SOLICITATION PROVISIONS AND CONTRACT CLAUSES

19. Amend section 52.204-9 by—

a. Revising the date of the clause; and

b. Removing from paragraph (d) "Federally-controlled information" and adding "Federal information" in its place.

The revision reads as follows:

52.204-9 Personal Identity Verification of Contractor Personnel.

* * * * *

PERSONAL IDENTITY VERIFICATION OF CONTRACTOR PERSONNEL (**DATE**)

* * * * *

20. Amend section 52.212-5 by—

a. Revising the date of the clause;

b. Redesignating paragraphs (b)(63) through (64) as paragraphs (b)(65) through (66);

c. Adding new paragraphs (b)(63) and (64);

d. Redesignating paragraph (e)(1)(xxiv) as paragraph (e)(1)(xxvi);

e. Adding new paragraphs (e)(1)(xxiv) and (xxv);

f. In Alternate II by—

i. Revising the date of Alternate II;

ii. Redesignating paragraphs (e)(1)(ii)(W) as paragraph (e)(1)(ii)(Y); and adding new paragraphs (e)(1)(ii)(W) and (X);

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-YY Federal Information Systems Using Non-Cloud Computing Services (**DATE**) (E.O. 14028 and 15 U.S.C. 278g-3e).

__ (64) 52.239-XX Federal Information Systems Using Cloud Computing Services (**DATE**) (E.O. 14028).

* * * * *

(e)(1) * * *

(xxiv) 52.239-YY Federal Information Systems Using Non-Cloud Computing Services (**DATE**) (E.O. 14028 and 15 U.S.C. 278g-3e).

(xxv) 52.239-XX Federal Information Systems Using Cloud Computing Services (**DATE**) (E.O. 14028).

* * * * *

Alternate II. (**DATE**) * * *

(e)(1) * * *

(ii) * * *

(W) 52.239-YY Federal Information Systems Using Non-Cloud Computing Services (**DATE**) (E.O. 14028 and 15 U.S.C. 278g-3e).

(X) 52.239-XX Federal Information Systems Using Cloud Computing Services (**DATE**)(E.O. 14028).

* * * * *

21. Amend section 52.213-4 by—

a. Revising the date of the clause;

b. Adding paragraphs (a)(1)(xii) and (xiii); and

c. Revising the date of paragraph (a)(2)(vii).

The additions and revisions 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**)

* * * * *

(a) * * *

(1) * * *

(xii) 52.239-YY Federal Information Systems Using Non-Cloud Computing Services (**DATE**)(E.O. 14028 and 15 U.S.C. 278g-3e).

(xiii) 52.239-XX Federal Information Systems Using Cloud Computing Services (**DATE**)(E.O. 14028).

(2) * * *

(vii) 52.244-6, Subcontracts for Commercial Products and Commercial Services (**DATE**).

* * * * *

22. Adding new sections 52.239-XX and 52.239-YY to read as follows:

52.239-XX Federal Information Systems Using Cloud Computing Services.

As prescribed in 39.X04(b) insert the following clause:

FEDERAL INFORMATION SYSTEMS USING CLOUD COMPUTING SERVICES (**DATE**)

(a) *Definitions*. As used in this clause—

Cloud computing means a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud computing is characterized by on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service; and includes service models such as software-as-a-service, infrastructure-as-a-service, and platform-as-a-service (NIST SP 800-145).

Federal information system—

(1) Means an information system (44 U.S.C. 3502(8)) used or operated by an agency, by a contractor of an agency, or by another organization, on behalf of an agency;

(2) *On behalf of an agency* as used in this definition, means when a contractor uses or operates an information system or maintains or collects information for the purpose of processing, storing, or transmitting Government data, and those activities are not incidental to providing a service or product to the Government (32 CFR part 2002).

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 with access 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 data means any information (including metadata), document, media, or machine-readable material regardless of physical form or characteristics that is created or obtained by the Government, or a contractor on behalf of the Government, in the course of official Government business.

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 primarily applied to the Government data.

Information means any communication or representation of knowledge, such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, electronic, or audiovisual forms (see Office of Management and Budget (OMB) Circular No. A-130, Managing Information as a Strategic Resource).

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.

Media means physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, large-scale integration memory chips, and printouts onto which information is recorded, stored, or printed within an information system (NIST SP 800-53).

(b) *Applicability*. The requirements of this clause shall only apply to aspects of a Federal information system (FIS) that involve cloud computing services.

(c) *Cloud computing security requirements*.

(1) The Contractor shall implement and maintain security and privacy safeguards and controls with the security level and services required in accordance with the Federal Risk and Authorization Management Program (FedRAMP) authorization level specified.

(i) Cloud continuous monitoring requirement. The Contractor shall engage in continuous monitoring activities and provide continuous monitoring deliverables as required for FedRAMP approved capabilities (see FedRAMP Continuous Monitoring Strategy Guide).

(ii) Cryptographic key services. The Government reserves the right to implement and operate its own cryptographic key management, key revocation and key escrow services.

(2) For cloud computing services required to meet FIPS Publication 199 high impact requirements, the Contractor shall maintain within the United States and its outlying areas (see FAR 2.101) all Government data that is not physically located on U.S. Government premises, unless otherwise specified in the contract.

(d) *Limitations on access to, and use and disclosure of, Government data and Government-related data*.

(1) The Contractor shall not access, use, or disclose Government data or Government-related data unless specifically authorized under the contract or task or delivery order or in writing by the Contracting Officer.

(i) When authorized, any access to, or use or disclosure of, Government data or Government-related data shall only be for purposes specified in the contract or task order or delivery order.

(ii) The Contractor shall ensure that its employees are subject to all such access, use, and disclosure prohibitions and obligations of this paragraph.

(iii) The access, use, and disclosure prohibitions and obligations of this paragraph shall survive the expiration or termination of this contract.

(2) The Contractor shall use Government-related data only to manage the operational environment that supports the Government data and for no other purpose unless otherwise permitted with the prior written approval of the Contracting Officer.

(e) *Notifiable incident reporting, incident response and threat reporting*.

For contract coverage on security incident and cyber threat reporting, see FAR clause 52.239-ZZ, Incident and Threat Reporting and Incident Response Requirements for Products or Services Containing Information and Communications Technology, in this contract.

(f) *Records management and Government access.*

(1) The Contractor shall provide the Contracting Officer with all Government data and Government-related data in the format specified in the contract.

(2) The Contractor shall dispose of Government data and Government-related data in accordance with the terms of the contract and provide the confirmation of disposition to the Contracting Officer in accordance with contract closeout procedures.

(3)(i) To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, (i.e., confidentiality, integrity, and availability) and privacy of Government data; or for the purpose of audits, investigations, inspections, or other similar activities, as authorized by law, regulation, or this contract, the Contractor shall provide the Government's authorized representatives (authorized representatives include CISA, except for contracts with the Department of Defense, the Intelligence Community, or for National Security Systems, and could include other Federal agencies, as specified by the Contracting Officer) with—

(A) Timely access, including full access, to all Government data and Government-related data;

(B) Timely access to contractor personnel involved in performance of the contract; and

(C) Specifically for the purpose of audit, investigation, inspection, or other similar activity, as authorized by law, regulation, or this contract, timely physical access to any Contractor facility with Government data.

(ii) In response to a request for access from CISA, the Contractor shall—

(A) First confirm the validity of the request by contacting CISA Central by email at report@cisa.gov, or by telephone at 888-282-0870; 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 under this clause shall not be delayed by submission of this notification or awaiting acknowledgement of its receipt.

(g) *Notification of third-party access requests*. The Contractor shall notify the Contracting Officer promptly of any requests from a third-party for access to Government data or Government-related data, including any warrants, seizures, or subpoenas it receives, including those from another Federal, State, or local agency. The Contractor shall comply with applicable clauses, regulations, and laws concerning protection of Government data and Government-related data from any unauthorized disclosure.

(h) *Indemnity for potential or actual loss or damage of Government data.*

(1) The Contractor shall indemnify the Government and its officers, agents, and employees acting for the Government against any liability arising out of the performance of this contract, including costs and expenses, incurred as the result of the Contractor's unauthorized introduction of copyrighted material to which the Contractor has no rights or license that may infringe on the copyright interest of others, information subject to a right of privacy, and any libelous or other unlawful matter into Government data. The Contractor agrees to waive any and all defenses that may be asserted for its benefit, including (without limitation) the "Government Contractors Defense."

(2) The Contractor shall indemnify the Government and its officers, agents, and employees acting for the Government against any liability arising out of the performance of this contract, including costs and expenses, incurred as the result of the Contractor's potential or actual unauthorized disclosure of trade secrets, copyrighted materials, contractor bid or proposal information, source selection information, classified information, material marked as "Controlled Unclassified Information", information subject to a right of privacy or publicity, personally identifiable information as defined

by OMB Circular A-130 (2016) or successor thereof, or any record as defined in 5 U.S.C. 552a.

(3) In the event of any claim or suit against the Government on account of any alleged unauthorized disclosure or introduction of data or information arising out of the performance of this contract or services performed under this contract, the Contractor shall furnish to the Government, when requested by the Contracting Officer, all evidence and information in the Contractor's possession pertaining to such claim or suit.

(4) The provisions of this paragraph (h) do not apply unless the Government provides notice to the Contractor as soon as practicable of any claim or suit, affords the Contractor an opportunity under applicable laws, rules, or regulations to participate in the defense of the claim or suit, and these provisions do not apply to any libelous or other unlawful matter contained in such data furnished to the Contractor by the Government and incorporated in data to which this clause applies. Further, this indemnity shall not apply to—

(i) A disclosure or inclusion of data or information upon specific written instructions of the Contracting Officer directing the disclosure or inclusion of such information or data;

(ii) A third-party claim that is unreasonably settled without the consent of the Contractor, unless

required by final decree of a court of competent jurisdiction.

(i) *Subcontracts*. The Contractor shall include the substance of this clause, including this paragraph (i), in all subcontracts under this contract for services to develop, implement, operate, or maintain a FIS using cloud computing services.

(End of clause)

52.239-YY Federal Information Systems Using Non-Cloud Computing Services.

As prescribed in 39.X04(a) insert the following clause:

FEDERAL INFORMATION SYSTEMS USING NON-CLOUD COMPUTING SERVICES (**DATE**)

(a) Definitions. As used in this clause—

Cloud computing means a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud computing is characterized by on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service; and includes service models such as software-as-a-service, infrastructure-as-a-service, and platform-as-a-service (NIST SP 800-145).

Component means a discrete identifiable information and operational technology asset that represents a building block of a system and may include hardware, software, and firmware.

Cyber supply chain risk means the potential for harm or compromise that arises as a result of cybersecurity risks from suppliers, their supply chains, and their products or services. This includes risks that arise from threats exploiting vulnerabilities or exposures within products and services traversing the supply chain as well as threats or exposures within the supply chain itself. The level of risk depends on the likelihood that relevant threats may exploit applicable vulnerabilities and the consequential potential impacts.(NIST SP 800-161 and 800-203).

Federal information system—

(1) Means an information system (44 U.S.C. 3502(8)) used or operated by an agency, by a contractor of an agency, or by another organization, on behalf of an agency;

(2) *On behalf of an agency* as used in this definition, means when a contractor uses or operates an information system or maintains or collects information for the purpose of processing, storing, or transmitting Government data, and those activities are not incidental to providing a service or product to the Government (32 CFR part 2002).

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 with access 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 data means any information, (including metadata), document, media, or machine-readable material regardless of physical form or characteristics that is created or obtained by the Government, or a contractor on

behalf of the Government, in the course of official Government business.

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 primarily applied to the Government data.

High value asset means Government data or a Federal information system that is designated as a high value asset pursuant to OMB Memorandum M-19-03, Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program.

Information means any communication or representation of knowledge, such as facts, data, or opinions, in any medium or form, including textual, numerical, graphic, cartographic, narrative, electronic, or audiovisual forms (see Office of Management and Budget (OMB) Circular No. A-130, Managing Information as a Strategic Resource).

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.

Information technology means any equipment, or interconnected system(s) or subsystem(s) of equipment, that is used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency.

(1) For purposes of this definition, equipment is used by an agency if the equipment is used by the agency directly or is used by a contractor under a contract with the agency that requires—

(i) Its use; or

(ii) To a significant extent, its use in the performance of a service or the furnishing of a product.

(2) The term "information technology" includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources.

(3) The term "information technology" does not include any equipment that—

(i) Is acquired by a contractor incidental to a contract; or

(ii) Is operational technology.

Internet of Things (IoT) devices means, consistent with section 2 paragraph 4 of Public Law 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.

Media means physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, large-scale integration memory chips, and printouts onto which information is recorded, stored, or printed within an information system (NIST SP 800-53).

Metadata means information describing the characteristics of data including, but not limited to, structural metadata that describes data structures (e.g., data format, syntax, and semantics) and descriptive metadata that describes data contents (e.g., information security labels) (NIST SP 800-37).

Operational technology (OT) 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).

Overlay means a specification of security or privacy controls, control enhancements, supplemental guidance, and other supporting information employed during the tailoring process, that is intended to complement and further refine security control baselines. An overlay specification may be more stringent or less stringent than the original security control baseline specification and can be applied to multiple information systems (OMB Circular No. A-130).

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) *Applicability*. The requirements of this clause shall only apply to aspects of a Federal information system (FIS) that do not involve cloud computing services.

(c) *Records management and Government access*.

(1) The Contractor shall provide the Contracting Officer with all Government data and Government-related data in the format specified in the contract.

(2) The Contractor shall dispose of Government data and Government-related data in accordance with the terms of the contract and provide the confirmation of disposition to

the Contracting Officer in accordance with contract closeout procedures.

(3)(i) To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security (i.e., confidentiality, integrity, and availability) and privacy of Government data; or for the purpose of audits, investigations, inspections, or other similar activities, as authorized by law, regulation, or this contract, the Contractor shall provide the Government's authorized representatives (authorized representatives include CISA, except for contracts with the Department of Defense, the Intelligence Community, or for National Security Systems, and could include other Federal agencies as specified by the Contracting Officer), with—

(A) Timely access, including full access, to all Government data and Government-related data;

(B) Timely access to contractor personnel involved in performance of the contract; and

(C) Specifically for the purpose of audit, investigation, inspection, or other similar activity, as authorized by law, regulation, or this contract, timely physical access to any Contractor facility with Government data.

(ii) In response to a request for access from CISA, the Contractor shall—

(A) First confirm the validity of the request by contacting CISA Central by email at report@cisa.gov, or by telephone at 888-282-0870; 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 under this clause shall not be delayed by submission of this notification or awaiting acknowledgement of its receipt.

(d) *Annual assessments*. (1) If the Contractor is required to develop, implement, operate, or maintain a FIS that is designated as a moderate or high Federal Information Processing Standards (FIPS) Publication 199 impact, the Contractor shall, unless otherwise stated in the contract—

(i) Perform an annual, independent assessment of the security of each FIS to include an architectural review and penetration testing of the FIS;

(ii) At least annually, conduct a cyber threat hunting and vulnerability assessment to search for cybersecurity risks, vulnerabilities and indicators of compromise;

(iii) Promptly provide the Contracting Officer with the results of the assessments at paragraphs (d)(1)(i) and (ii) of this clause, including any recommended improvements or risk mitigations for each FIS;

(iv) Upon agency request, promptly implement the recommended improvements and mitigations, if any, for the FIS; and

(v) For any recommendation the agency does not request be implemented, document the agency-provided rationale for not implementing the improvement or mitigation in the Contractor's System Security Plan (SSP).

(2) If the Contractor contracts with a third-party assessment organization to perform the assessments required in paragraph (d)(1)(i) and (ii) of this clause, the Contractor shall enter into a strict confidentiality agreement with the third-party assessment organization. The Contractor shall notify the Contracting Officer of any existing business relationships the Contractor has with the third-party assessment organization. The confidentiality agreement shall—

(i) Ensure compliance with all applicable requirements for disclosing information to the Government; and

(ii) Prohibit the third-party assessment organization from—

(A) Disclosing any Government data, and

(B) Retaining on its systems any Government data following the conclusion of the assessment and transfer of all information related to the assessment results to the Contractor.

(e) *Security and privacy controls.*

(1) The Contractor shall implement the controls, as specified by the agency, in—

(i) National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Security and Privacy Controls for Information Systems and Organizations;

(ii) NIST SP 800-161, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations;

(iii) NIST SP 800-82, Guide to Industrial Control Systems Security; and

(iv) NIST SP 800-213, IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements.

(2) The Contractor shall implement any additional requirements, as identified in the contract, for an information system designated by the agency as a high value asset. These requirements may include implementation of a high value asset overlay and cooperation in the conduct of all required cybersecurity assessments.

(3) The security and privacy controls specified by the agency in accordance with paragraph (e)(1) of this section will include a requirement to develop, review, and update, if appropriate, an SSP to support authorization of all applicable FIS.

(i) NIST SP 800-18, Guide for Developing Security Plans for Federal Information Systems, contains a template for an Information SSP; and

(ii) The Contractor shall submit a copy of the SSP to the agency upon request.

(4) The Contractor shall make contingency plans for all information systems, aligned to NIST SP 800-34, Contingency Planning Guide for Federal Information Systems, available to the agency upon request.

(5) For a FIS required to meet FIPS Publication 199 high impact requirements, the Contractor shall maintain within the United States and its outlying areas (see FAR 2.101) all Government data that is not physically located on U.S. Government premises, unless otherwise specified in the contract.

(f) *Additional considerations*. For each FIS being developed, implemented, operated, or maintained, the Contractor shall-

(1) Apply NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View, as the basis for the Contractor's risk management process (framing, assessing, responding to, and monitoring risk) when supporting agency risk management activities;

(2) Apply NIST SP 800-37, Risk Management Framework for Information Systems and Organizations: A System Life

Cycle Approach for Security and Privacy, as the process to manage system risk through preparation, categorization, control selection, control implementation and assessment, system authorizations, and continuous monitoring;

(3) Apply NIST SP 800-207, Zero Trust Architecture, when designing zero trust architecture approaches;

(4) Apply NIST SP 800-160, Vol. 1, Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems, which addresses the activities and tasks, the concepts and principles, and most importantly, what needs to be considered from a security perspective when executing within the context of systems engineering;

(5) Apply NIST SP 800-160, Vol. 2, Developing Cyber-Resilient Systems: A Systems Security Engineering Approach, when selecting, adapting, and using cyber resiliency constructs for new systems, system upgrades, or repurposed systems;

(6) Apply NIST SP 800-30, Guide for Conducting Risk Assessments, when preparing for, conducting, communicating results from, and maintaining risk assessments over time;

(7) Provide the Government with a continuous monitoring strategy for the FIS that maintains ongoing awareness of information security, vulnerabilities, and threats, in order to support organizational risk management decisions, and applies the following—

(i) NIST SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, which describes development and implementation of an ISCM Program, including development of an ISCM strategy;

(ii) Use of automation, wherever possible, to increase the speed, effectiveness, and efficiency of continuous monitoring; and

(iii) Protection of vulnerability scan data, logs, and telemetry data (e.g., from Cybersecurity and Infrastructure Security Agency's (CISA) Continuous Diagnostics and Mitigation program) commensurate with the aggregate sensitivity of the collected data. The data and logs shall be promptly made available to the Government upon the Contracting Officer's request;

(8) Apply NIST SP 800-63-3, Digital Identity Guidelines, when—

(i) Selecting appropriate digital identity services;

(ii) Digitally authenticating a subject to Federal information systems over a network; and

(iii) Implementing identity assurance, authenticator assurance, and federation assurance levels based on risk; and

(9) Apply NIST SP 800-92, Guide to Computer Security Log Management, when generating, transmitting,

storing, analyzing, and disposing of computer security log data.

(g) *Cyber supply chain risk management*. The Contractor may implement alternative, additional, or compensating cyber supply chain risk management security controls from those stated in the contract, when authorized in writing by the Contracting Officer.

(h) *Notifiable incident reporting, incident response and threat reporting*.

For contract coverage on security incident and cyber threat reporting, see FAR clause 52.239-ZZ, Incident and Threat Reporting and Incident Response Requirements for Products or Services Containing Information and Communications Technology, in this contract.

(i) *Limitations on access to, use, and disclosure of Government data, Government-related data, and any associated metadata*.

(1) The Contractor shall not access, use, or disclose Government data, Government-related data, and any associated metadata unless specifically authorized under the contract or task or delivery order or in writing by the Contracting Officer.

(i) When authorized, the access, use, or disclosure of Government data, Government-related data, and any associated metadata shall only be for purposes specified in the contract or task or delivery order.

(ii) The Contractor shall ensure that its employees are subject to all such access, use, and disclosure prohibitions and obligations of this paragraph.

(iii) The access, use, and disclosure prohibitions and obligations of this paragraph shall survive the expiration or termination of this contract.

(2) The Contractor shall use Government metadata only to manage the operational environment that supports the Government data and for no other purpose unless otherwise permitted with the prior written approval of the Contracting Officer.

(3) The Contractor shall notify the Contracting Officer promptly of any requests from a third-party for access to Government data, Government-related data, or any associated metadata, including any warrants, seizures, or subpoenas it receives, including those from another Federal, State, or local agency. The Contractor shall comply with applicable clauses, regulations, and laws concerning protection of Government data and Government-related data from any unauthorized disclosure.

(4) The Contractor shall not publish or disclose in any manner, without the Contracting Officer’s written consent, the details of any safeguards either designed or developed by the Contractor under this contract or otherwise provided by the Government.

(j) *Cryptographic key services.* The Government reserves the right to implement and operate its own cryptographic key management, key revocation, and key escrow services. If key services are provided by the contractor, the contractor shall provide the agency with applicable key material and services.

(k) *List of operational technology equipment.* Unless the contract states otherwise, the Contractor shall develop and maintain a list of the physical location of all operational technology included within the boundary of a FIS covered by this contract.

(1) The list shall be considered Government data. At a minimum, the list shall include—

(i) The identification and description of any controllers, relays, sensors, pumps, actuators, Open Platform Communications Unified Architecture devices, and other industrial control system devices; including, when available, the manufacturer, part number, software version, communication protocols, and all static IP addresses assigned to the different hardware components used in performance of the contract;

(ii) An explanation of whether the device is password protected and, if so, whether the password can be changed from the default password provided by the manufacturer;

(iii) An explanation of whether the device is accessible remotely (e.g., through internet or another network connection);

(iv) Location information in enough detail to affirmatively locate the operational technology equipment, if necessary; and

(v) Whether multi-factor authentication is present and enabled.

(2) The Contractor shall update the list to track any movement of the equipment during contract performance, as software or firmware updates are applied, when equipment is removed or taken out of service; or when equipment is added or placed into service.

(3) Upon request by the Contracting Officer, the Contractor shall provide the Government a copy of the current and/or historical list(s).

(l) *Binding Operational Directives and Emergency Directives.*

(1) Except as identified in paragraph (l)(2) of this clause, the Contractor shall comply with the Binding Operational Directives (BODs) and Emergency Directives (EDs) issued by CISA and having a specific applicability to a FIS used or operated by a contractor. The list of BODs and EDs can be found at *https://www.cisa.gov/directives*.

(2) The following BODs and EDs that have a specific applicability to a FIS used or operated by a contractor will not apply to this contract: _____.

[*Contracting Officer to list any BODs or EDs not applicable to the contract, as specified by the requiring activity*]

(3) BODs and EDs with specific applicability to a FIS used or operated by a contractor that are issued after the date of award will be applied to this contract, at the Contracting Officer's discretion, through appropriate modification of the contract.

(m) *Indemnity for potential or actual loss or damage of Government data.*

(1) The Contractor shall indemnify the Government and its officers, agents, and employees acting for the Government against any liability arising out of the performance of the contract, including costs and expenses, incurred as the result of the Contractor's unauthorized introduction of copyrighted material to which the Contractor has no rights or license that may infringe on the copyright interest of others, information subject to a right of privacy, and any libelous or other unlawful matter into Government data. The Contractor agrees to waive any and all defenses that may be asserted for its benefit, including (without limitation) the "Government Contractors Defense."

(2) The Contractor shall indemnify the Government and its officers, agents, and employees acting for the Government against any liability arising out of the performance of this contract, including costs and expenses, incurred as the result of the Contractor's potential or actual unauthorized disclosure of trade secrets, copyrighted materials, contractor bid or proposal information, source selection information, classified information, material marked as "Controlled Unclassified Information", information subject to a right of privacy or publicity, personally identifiable information as defined by OMB Circular A-130 (2016) or successor thereof, or any record as defined in 5 U.S.C. 552a.

(3) In the event of any claim or suit against the Government on account of any alleged unauthorized disclosure or introduction of data or information arising out of the performance of this contract or services performed under this contract, the Contractor shall furnish to the Government, when requested by the Contracting Officer, all evidence and information in the Contractor's possession pertaining to such claim or suit.

(4) The provisions of this paragraph (m) do not apply unless the Government provides notice to the Contractor as soon as practicable of any claim or suit, affords the Contractor an opportunity under applicable laws, rules, or regulations to participate in the defense

of the claim or suit, and these provisions do not apply to any libelous or other unlawful matter contained in such data furnished to the Contractor by the Government and incorporated in data to which this clause applies. Further, this indemnity shall not apply to—

(i) A disclosure or inclusion of data or information upon specific written instructions of the Contracting Officer directing the disclosure or inclusion of such information or data; or

(ii) A third-party claim that is unreasonably settled without the consent of the Contractor, unless required by final decree of a court of competent jurisdiction.

(n) *Subcontracts*. The Contractor shall include the substance of this clause, including this paragraph (n), in all subcontracts under this contract for services to develop, implement, operate, or maintain, a FIS using other than cloud computing services.

(End of clause)

23. Amend section 52.244-6 by—

a. Revising the date of the clause; and

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

The revisions 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-YY Federal Information Systems Using Non-Cloud Computing Services (**DATE**) (E.O. 14028 and 15 U.S.C. 278g-3e) if flow down is required in accordance with paragraph (n) of FAR clause 52.239-YY.

(xxii) 52.239-XX Federal Information Systems Using Cloud Computing Services (**DATE**) (E.O. 14028) if flow down is required in accordance with paragraph (i) of FAR clause 52.239-XX.

* * * * *

[FR Doc. 2023-21327 Filed: 10/2/2023 8:45 am; Publication Date: 10/3/2023]