THE
COALITION
FOR GOVERNMENT PROCUREMENT

February 2, 2024

Marissa Ryba
Procurement Analyst
Regulatory Secretariat Division
General Services Administration
1800 F St. NW
Washington, DC 20405

Re: FAR Case 2021-017, "Federal Acquisition Regulation: Cyber Threat and Incident Reporting and Information Sharing"

Ms. Ryba:

The Coalition for Government Procurement ("the Coalition") appreciates the opportunity to submit these comments on the above-referenced proposed rule, "Federal Acquisition Regulation: Cyber Threat and Incident Reporting and Information Sharing."

By way of background, the Coalition is a non-profit association of firms selling commercial services, products, and solutions to the Federal Government. Our members collectively account for tens of billions of dollars of the sales generated through the GSA Multiple Award Schedules (MAS) program, VA Federal Supply Schedules (FSS), the Government-wide Acquisition Contracts (GWACs), and agency-specific multiple award contracts (MACs). Coalition members include small, medium, and large businesses that account for more than $145 billion in Federal Government contracts. The Coalition is proud to have worked with Government officials for more than 40 years towards the mutual goal of common-sense acquisition.

The Coalition strongly supports the underlying objective of the proposed rule to strengthen Federal cybersecurity and protect Government networks by standardizing and partially centralizing Government and industry responses to cyber incidents and threats. As we noted in testimony before the House Subcommittee on Cybersecurity, Information Technology, and Government Innovation last year, however, unnecessarily burdensome cybersecurity requirements drive companies out of the Government marketplace, hampering agency access to innovation needed to meet their missions and leaving Government less, not more, secure.[1] To address this potential unintended consequence, the Coalition makes the following comments pertaining to the:

- Scope of the clause;
- Definition of "security incident;"
- Proposed reporting time frame;

[1] Statement of Roger D. Waldron, President of the Coalition for Government Procurement, November 29, 2023, https://oversight.house.gov/wp-content/uploads/2023/11/Final-Testimony-Roger-Waldron.pdf.

- Requirement to provide Software Bills of Materials (SBOMs);
- Subcontracting;
- Waiver process;
- Federal Bureau of Investigation (FBI)/Cybersecurity and Infrastructure Security Agency (CISA) access requirements; and
- The Security Incident Reporting Representation provision.

We have indicated where these comments respond to the specific questions raised in the proposed rule.

Scope and Applicability of the Incident and Threat Reporting and Response Clause

The Coalition's first comment concerns the scope and impact of the proposed clause, FAR 52.239-ZZ, "Incident and Threat Reporting and Incident Response Requirements for Products or Services Containing Information and Communications Technology [ICT]," set to be included in all contracts. In the proposed rule, it is estimated that 75 percent of all Federal contractors (70,526 entities annually awarded contracts) have contracts with some information and communications technology, and thus, would be impacted by the rule.

Any rule on incident reporting and response would affect a significant number of contractors. For this reason, the Coalition recommends that the FAR Council clarify the scope of applicability by explaining what qualifies as using or providing ICT in the performance of the contract and limit application of the clause for procurements under Part 39, aligning to definitions (and noted exemptions) in FAR 2.101 for ICT and Information Technology. This will ensure contractors and offerors clearly understand their cybersecurity obligations under applicable contracts.

Definition of a "Security Incident"

The proposed clause defines a security incident as the "actual or potential occurrence of the following—

> (1) Any event or series of events, which pose(s) actual or imminent jeopardy, without lawful authority, to the integrity, confidentiality, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies;
>
> (2) Any malicious computer software discovered on an information system; or
>
> (3) Transfer of classified or controlled unclassified information onto an information system not accredited (*i.e.*, authorized) for the appropriate security level."

Recognizing that the first provision of this definition is based on existing US authorities regarding the coordination of Federal information policy,[2] we appreciate the Council's apparent effort to maintain consistency across Federal cybersecurity policy.

The reference to an "actual or potential" occurrence should be removed to eliminate some of the ambiguity associated with the definition, which further defines a security incident to include events that pose "actual or imminent jeopardy." This narrows the definition somewhat and will help reduce over-reporting by contractors. Additional guidance for contractors with respect to the definition as well as including a materiality element and a greater focus on the effects of the events would be useful to ensure incident reporting achieves its intended purpose. An unintended consequence of the proposed rule, as currently written, will likely be both over- and under-reporting by contractors. In an (over) abundance of caution, some contractors may choose to report potential occurrences that have a very low probability of having jeopardized an information system, or whose potential effect on the security of the system is very slight. Such overreporting risks negatively affecting the utility of the CISA Incident Reporting System, fatiguing staff at the contracting agency, and diverting contractors' cybersecurity staff away from substantive security work towards compliance exercises of questionable value. Other contractors, however, may set a higher bar than the Government desires for what qualifies as a potential occurrence and fail to report security incidents as often as the Government had hoped.

Thus, we recommend that the Council include additional language to clarify at what level a potential occurrence is considered reportable by the contractor. Because compliance with the rule is material to eligibility and payment, and non-compliance with the rule opens contractors to liability under the False Claims Act, clarity is needed to reassure contractors that their good-faith efforts to comply with the rule will be acceptable.

Paragraph (3) of the rule should be removed. If paragraph (3) is retained, Coalition members seek clarification about how paragraph (3) is intended to operate with the requirement that reports take place through CISA's Cyber Incident Reporting system, which is not rated for the transfer of classified information or controlled unclassified information. To the extent that reporting may implicate that information or how it is safeguarded, contractors may be unable to comply with the rule's reporting requirement. Further, if paragraph (3) is retained, we suggest the following modifications. First, paragraph (3) should not address classified information, as classified information is appropriately addressed under NISPOM. Second, with respect to CUI, FAR and DFARS rules have not yet been finalized to clarify requirements for contractor information system accreditation. Paragraph (3) should distinguish between transfer to systems owned and controlled by the contractor (which can be easily remedied without the need for reporting and which does not pose a material risk of compromise), and transfer to systems not controlled by the contractor.

[2] 44 USC § 3552 (b)(2).

Beyond the present rulemaking effort, Coalition members suggest that the Government harmonize definitions of terms like "security incident" and "cybersecurity incident" across the DFARS, HSAR, the Federal Authorization and Risk Management program (FedRAMP) and the pending rule implementing the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA).

Harmonizing Incident Reporting for Cloud Service Providers

Because FedRAMP already has incident communications procedures in place that are substantially similar to those envisioned by the rule, the Coalition recommends that cloud service providers (CSPs) with a FedRAMP authorization be exempted from the rule's reporting requirements with respect to incidents relating to the FedRAMP authorized environment so long as they comply with FedRAMP's incident communications procedures.

Improving the Submission of CISA Incident Reports

We recommend that the FAR Council work with CISA to make the following adjustments to improve the Cybersecurity Incident Reporting system's utility for Federal contractors:

- The Government should allow report submission via application programming interface (API) in addition to manual reporting via the CISA portal. Contractors that submit reports via API should not be required to submit using the manual electronic form.
- The fields within the CISA electronic form are ambiguous. Words and terms within the form need to be defined to allow contractors to understand and provide the appropriate response. For example, the primary CI sector is unclear. Additionally, context should be given for the fields as well, *e.g.* "Private Sector - Not Critical Infrastructure Aligned; or Information Technology" requires specification regarding the company type. It is unclear whether the aforementioned field is meant for all types of private industry technology companies.
- Additionally, many of the fields are not required for all contractors when reporting an availability incident. We recommend CISA reassess and consider all contractor types (*e.g.,* small business contractors, package software providers, cloud service offerings).

Time Frame for the Reporting of Cyber Incidents

The proposed clause's (FAR 52.239-ZZ) eight-hour reporting requirement also may result in a high incidence of false positive reporting which could unnecessarily add to the workload of the Government's already limited cybersecurity workforce. Coalition members report that an eight-hour time frame for reporting incidents is insufficient to understand the facts on the ground, such as the degree of potential harm associated with the incident and the likelihood that a potential occurrence creates actual or imminent jeopardy.

For this reason, we recommend that the Council harmonize the proposed rule with the 72-hour requirement established by the DFARS and the CIRCIA to provide the contractor more time to conduct its initial investigation, prepare a preliminary report, and begin remediation. Beyond the present rule making effort, we encourage, to the extent possible, harmonization of time frames for reporting across all agency regulations, including the DFARS, HSAR, and the pending rule implementing the CIRCIA. Although different systems may have different cybersecurity needs, consistency across agencies should be achieved to the maximum extent practicable, as it can minimize the number of standards contractors face and, thereby, mitigate compliance confusion.

Software Bill of Materials

We recommend requirements in the proposed rule related to SBOMs be removed as outside the scope of the proposed rule, which is meant to address cyber threat and incident reporting and information sharing. Further, software supply chain security, per Executive Order 14028, is being addressed in a separate rulemaking (FAR Case 2023-002). To the extent SBOM requirements are retained, please see below comments in response to questions posed in the proposed rule.

How should SBOMs be collected from contractors? What specific protections are necessary for the information contained within an SBOM?

The Coalition recommends that SBOMs be provided directly to the Government in a secure manner and stored centrally. A public website that contains SBOMs creates potential security vulnerabilities, including placing proprietary intellectual property SBOMs may contain at risk, potentially undermining contractor incentive to participate in the Government market. Even if they are not public, however, centrally stored SBOMs without guaranteed technical safeguards create risks. If exposed, they give malicious actors significant information to help target their vulnerability discovery work. This would introduce a new risk to the software ecosystem. If the government does move forward with collecting SBOMs from all contractors, the government must provide proper access controls, encryption at rest, and assume liability in the event disclosure to non-authorized actors causes harm to the provider of the SBOM.

A public *listing* of submitted SBOMs, however, would be desirable so that contractors purchasing or reselling software simply would request such information from developers where a current SBOM was not submitted. Contractors also could refer agencies to this list when they needed to obtain the SBOM, realizing a time-saving “do once, use many” model for developers, contractors, and agencies.

We recommend that SBOMs not be collected for cloud service offerings, as they are subject to frequent change, and the Cloud Service Provider (CSP), rather than the end user, is responsible for applying required security updates, based on information contained in the SBOM.

Rather, to accomplish the government’s goal of encouraging the private sector to “adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace” the government should allow CSPs to demonstrate their maintenance of software provenance through FedRAMP, with verification from a 3PAO. One option would be to allow CSPs to select NIST SP800-53 Rev. 5, SR-4 Provenance control into their baselines.

How should the Government think about the appropriate scope of the requirement on contractors to provide SBOMs to ensure appropriate security?

As written, the FAR clause implies that any software used requires an SBOM. This requirement could limit the ability of contractors to use the best commercial software to satisfy a particular contract and lead to the submission of a large number of SBOMs with little practical value to the Government. We recommend that the FAR clause clarify the circumstances when an SBOM would be required (*e.g.,* for on-prem software installed on a Government system or software that is delivered to the Government in performance) and circumstances where it would not be required (*e.g.,* use of standard back-office software application, such Microsoft Excel or Word, to generate reports or spreadsheets).

We further recommend that the Government start with a pilot program to collect SBOMs only for packaged software, while allowing cloud offerings to demonstrate software provenance through FedRAMP as mentioned above. The Government could evaluate the security benefit of the collection of SBOMs for packaged software, along with the efficacy of allowing CSPs to demonstrate their software provenance tracking through the FedRAMP Program, before imposing SBOM collection requirements on cloud service offerings.

When monitoring SBOMs (or software provenance data) for embedded software vulnerabilities as they are discovered, Cloud Service Providers should provide the government with assurance, through a 3PAO, they have in place:

1) A software provenance tracking system,

2) A vulnerability management process, and

3) An incident response plan.

The Government's role would be to regularly verify that these systems and processes are in place through the FedRAMP Program.

What challenges will contractors face in the development of SBOMs? What challenges are unique to software resellers? What challenges exist regarding legacy software?

Coalition members identify the following challenges, categorized per question.

General Challenges:

- SBOM generation is largely manual with limited automated tools to assist. Software vendors will have security concerns if required to share SBOMs with the Government and/or third-party companies who may also be competitors.
- Clearly delineating the relationship between software packages that rely on other packages is challenging but important to accuracy. Because open-source packages are highly leveraged, the risk of bad data within the SBOM increases.

- For cloud service offerings, the code is updated many times a day (up to hundreds of times). So, there will be challenges in the volume of SBOMs produced, and there is no efficient way to provide the government with daily updates of the SBOMs. This is why it is better to leverage the FedRAMP Program, which CSPs must adhere to in order to provide cloud services to the U.S. government, to verify that a CSP maintains software provenance rather than collecting SBOMs.
- SBOMs only provide value to a user if they have the agency to update the software and/or change its configuration to mitigate the identified risk.

Challenges unique to software resellers:

- It is unclear whether software resellers will be expected to establish and maintain their own SBOM repositories. In any event, there will be increased cost to software resellers who will need to establish processes to verify that software producers have satisfied SBOM requirements.
- Resellers will need to be a part of the security information chain with agencies and providers to communicate risks identified.

Legacy software:

- End of life applications are susceptible to exploitable weaknesses and without vendor support for legacy software. The government may lack the resources to patch and maintain legacy software.

What are the appropriate means of evaluating when an SBOM must be updated based on changes in a new build or major release?

Just like other security documentation, such as System Security Plans (SSPs), SBOMs should be updated often to maintain the accuracy of the data. We recommend that the rule provide a definition of “major release” or “new build” to ensure understanding as to when this applies.

What is the appropriate balance between the Government and the contractor, when monitoring SBOMs for embedded software vulnerabilities as they are discovered?

As a practice, large business contractors monitor their software for defects and vulnerabilities. This may not be feasible for small businesses, which is why it is important to clarify the scope of software uses that require an SBOM and monitoring of software vulnerabilities.

Subcontracting

Prime contractors may face significant challenges obtaining compliance from subcontractors, including, in particular, manufacturers and suppliers of FDA regulated products and software vendors of commercially available off-the-shelf (COTS) products. Indeed, the flowdown and subcontractor elements of 52.239-ZZ and 52.239-AA present unique and potentially untenable compliance obligations for COTS providers.

For many commercial software developers, the Federal market represents a negligible portion of their business. They may not structure compliance regimes around their products as set forth in the proposed rule; or their Federal market business share of their overall business mix may not be significant enough to justify incurring the additional cost of providing an SBOM to a reseller or to the Government.

For commercial vendors, including vendors of FDA regulated products, feasible supply alternatives may simply not exist, creating significant risk of diminished agency user and beneficiary access to innovation, including patient access to life saving products. When or if alternatives do exist, changes to the existing supply chain may prompt regulatory filings, which can take significant time to effectuate, presenting significant conflicts with the obligations under these clauses and again creating potential access issues. Given the representations and expectations associated with these clauses, a COTS manufacturer may be unable to negotiate these clauses into upstream agreements and therefore would be unable to comply or represent compliance. Moreover, the risk for non-compliance down the supply chain is on the prime exclusively, notwithstanding the fact that it may have limited-to-no control down that chain.

For this reason, to the maximum extent practicable, contractors and subcontractors should not be required to apply any clause to a subcontractor or supplier providing commercial products or services except those that include commercial products and services in their offerings. Those supplying commercial products or services should not be required to adhere to any clause except those applicable by law to subcontractors providing commercial products or services or those that are consistent with customary commercial practice.

In accordance with applicable statutory and regulatory requirements, we request that the Council consider whether it can: (1) exclude COTS products from full and applicability, (2) exclude subcontractors from flowdown requirements, or (3) consider whether a waiver process is appropriate to ensure access to products or software where compliance is not possible. In addition, we recommend that the Council engage the commercial industrial base to devise a compliance construct whereby the sought compliance with cyber integrity can be achieved in a manner that does not result in placing inordinate, if not near exclusive, risk on the prime contractor.

Shared Responsibility in the Cloud Market consistent with Commercial Practice

Additionally, government contractors increasingly depend on the support of cloud service providers (CSP) for a vast array of information and communications technology. To the extent requirements from the proposed rule are flowed to CSPs, the model that the clause envisions runs up against existing commercial best practices and the shared responsibility model for cybersecurity risk management.

In the shared responsibility model, a CSP is responsible for protecting the infrastructure that runs all of the services offered in the cloud, which includes the hardware, software, networking, and facilities delivered by the CSP. The organization (*i.e.,* the CSP's customer) is responsible for choosing the appropriate services and properly configuring and managing them to achieve the needed security outcomes. The organization's responsibility will vary based on the services they choose, the integration of those services into their IT environment, and applicable laws and regulations.

Security incidents can occur on either side of the shared responsibility model. Reporting requirements, however, should ensure that CSPs and their customers are only responsible for reporting incidents and managing data that occur on their respective sides of the shared responsibility model to avoid disrupting existing cybersecurity practice. For example, the data preservation requirements detailed in (c)(1)(i) of FAR clause 52.239-ZZ could require a contractor to infringe upon their customers' rights and responsibility in accordance with the shared responsibility model.

IPv6 Requirement

The Coalition recommends promoting harmonization across the government by aligning the IPv6 requirement in the proposed rule with the FedRAMP IPv6 requirement.

Access to Contracting Information and Information Systems

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

For any specific concerns identified, are there any specific safeguards, including safeguards that would address the scope of full access or how full access would be provided, that would address your concerns while still providing the Government with appropriate access to conduct necessary forensic analysis regarding security incidents?

Subparagraph (g)(i)(C) of section 2 of E.O. 14028 recognizes the need to identify appropriate and effective protections for privacy and civil liberties. Are there any specific safeguards that should be considered to ensure that these protections are effectively accomplished?

We understand that law enforcement agencies, like the FBI, and CISA would require full access to information, equipment, and contractor personnel. However, it is unclear why the contracting agency would require such access. Full access as described in the proposed rule should be restricted to law and security agencies whose mission is consistent with conducting such investigations.

Security Incident Reporting Representation

The proposed rule includes a representation provision, FAR 52. 52.239-AA, *Security Incident Reporting Representation*, that is to be inserted in all solicitations per FAR 39.108(c). As discussed above relating to the clause at FAR 52.239-ZZ, scope and applicability of the representation provision needs to be clarified as this provision opens contractors up to potential False Claims Act liability. The rule should include an opt-out mechanism for the contractor to represent whether the contractor provides or uses ICT, similar to cloud computing in DFARS 252.239-7009. With respect to the security incident reporting representation at part (b)(1), it should be made clear that the requirement to report security incidents runs prospectively from the date the clause is in the contract. For example, if a contract is modified to include FAR 52.239-ZZ, a contractor would not be required to report security incidents that occurred prior to the date of the modification.

Thank you again for the opportunity to submit these comments on FAR Case 2021-017, "Federal Acquisition Regulation: Cyber Threat and Incident Reporting and Information Sharing." To increase their utility, we have included an Appendix with suggested changes to FAR 52.239-ZZ, set in red text, alongside explanations for each change. The Appendix follows on the next page. If you have any questions, please contact me at rwaldron@thecgp.org or (202) 331-0975.

Best regards,

Roger Waldron
President

Appendix I: FAR 52.239-ZZ Proposed Edits & Comments

Proposed Rule w/ Edits	Comments
(a) Definitions. As used in this clause— *Active storage* means storing data in a manner that facilitates frequent use and ease of access.	
Cold data storage means storing data in a manner that minimizes costs while still allowing some level of access and use.	
Computer software (1) Means— (i) Computer programs that comprise a series of instructions, rules, routines, or statements, regardless of the media in which recorded, that allow or cause a computer to perform a specific operation or series of operations; and (ii) Recorded information comprising source code listings, design details, algorithms, processes, flow charts, formulas, and related material that would enable the computer program to be produced, created, or compiled. (2) Does not include computer databases or computer software documentation.	
Cyber threat indicators, in accordance with 6 U.S.C. 1501, means information that is necessary to describe or identify— (1) Malicious reconnaissance, including anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or security vulnerability; (2) A method of defeating a security control or exploitation of a security vulnerability; (3) A security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability; (4) A method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability; (5) Malicious cyber command and control;	

(6) The actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat; (7) Any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law; or (8) Any combination thereof.	
Defensive measures means an action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that is designed to detect, prevent, or mitigate a known or suspected cybersecurity threat or security vulnerability. The term “defensive measures” does not include a measure that destroys, renders unusable, provides unauthorized access to, or substantially harms an information system or information stored on, processed by, or transiting such information system not owned by the private entity operating the measure; or by another entity or Federal entity that is authorized to provide consent and has provided consent to that private entity for operation of such measure (6 U.S.C. 1501(7)).	This definition should focus more on the intent/design of defensive measures, as opposed to their efficacy. See proposed revision.
Eradication means reasonable efforts designed to eliminate or resolve the known mechanisms, components, and cause(s) of the incident, (such as deleting malware and disabling breached user accounts), as well as reasonable efforts designed to identify all affected known hosts within information systems and mitigating all known exploited vulnerabilities.	The focus of this definition should be on effort and intent, rather than efficacy. See proposed revisions.
Event means any observable occurrence in a system or network.	
Full access means, for all contractor information systems used in performance, ~~or which support performance~~, of the contract— (1) ~~Physical and~~ electronic access to— (i) Contractor networks, (ii) Systems, (iii) Accounts dedicated to Government systems only, ,[section iv deleted]	Please clarify the meaning of “used in performance” and “support performance”, and how they differ? This provision is unreasonably broad in a number of ways and should be limited to align with similar provisions such as in DFARS 252.204-7012. In particular, access to systems that “support performance” could potentially encompass all of a contractor’s systems. Access should be limited to the systems dedicated to the government contract or

(v) Other infrastructure with a shared identity boundary or interconnection to the Government system; and (2) If available, provision of all requested Government data or Government-related data, including relevant — (i) Images, (ii) Log files, (iii) Event information, and [section iv deleted]	housing government data. Further, permitting this level of access could put contractors in conflict with their contractual obligations and policies concerning confidentiality and privacy. See proposed revisions.
Government-related data means any information, document, media, or machine-readable material regardless of physical form or characteristics that is created or obtained by a contractor through the storage, processing, or communication of Government data. Government-related data does not include— (1) A contractor's business records (*e.g.*, financial records, legal records) that do not incorporate Government data, or (2) Data such as operating procedures, software coding or algorithms that are not uniquely applied to the Government data.	
Information and communications technology (ICT) means information technology and other equipment, systems, technologies, or processes, for which the principal function is the creation, manipulation, storage, display, receipt, or transmission of electronic data and information, as well as any associated content. Examples of ICT include but are not limited to the following: Computers and peripheral equipment; information kiosks and transaction machines; telecommunications equipment; telecommunications services; customer premises equipment; multifunction office machines; computer software; applications; websites; Internet of Things (IoT) devices; and operational technology.	Inclusion of “electronic media” and “electronic documents” makes this definition unreasonably broad and would result in virtually every contract being one which involves using or providing ICT. See proposed revisions which remove these terms from the definition.

Information system means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (44 U.S.C. 3502(8)). Information resources, as used in this definition, includes any ICT.	
Operational technology means programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems or devices detect or cause a direct change through the monitoring and or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms (NIST SP 800–160).	
Security incident means occurrence of an event or series of events, to the extent that it poses actual or imminent jeopardy to systems dedicated to storing, processing, or transmitting government data, or any government data contained therein.	This definition is unnecessarily broad and would result in CISA being inundated with reports of events that do not pose a significant risk. Recommend including a materiality element and a greater focus on the effects of the events. If part (3) is retained, it should be modified in two ways. First, it should not address classified information, as classified information is appropriately addressed under NISPOM. Second, with respect to CUI, it should distinguish between transfer to non-accredited systems owned and controlled by the contractor (which can be easily remedied without the need for reporting and which does not pose a material risk of compromise), and transfer to systems not controlled by the contractor. See proposed revisions.
Software bill of materials (SBOM) means a list of names of third-party open source software components as generated by a software composition analysis tool.	References to SBOM should be removed in their entirety as outside the scope of the proposed rule. If references to SBOM are retained, this definition is not consistent with industry standards. See the proposed definition which better aligns with common understanding and industry standards.

	If the current definition of SBOM is retained, please clarify what is meant by a “formal” record and “supply chain relationships.”
Supplier's declaration of conformity means a standardized format to document the USGv6 capabilities supported by a specific product or set of products and provides traceability back to the accredited laboratory that conducted the tests (see NIST SP 500–281B).	
Telecommunications equipment means equipment used to transmit, emit, or receive signals, signs, writing, images, or sounds, by wire, cable, satellite, fiber optics, laser, radio, or any other electronic, electric, electromagnetic, or acoustically coupled means.	The phrase “or intelligence of any nature” should be stricken from the definition, as it is ambiguous and extremely broad. In the alternative, please clarify what the phrase means.
Telecommunications services means services used to transmit, emit, or receive signals, signs, writing, images, or sounds, by wire, cable, satellite, fiber optics, laser, radio, or any other electronic, electric, electromagnetic, or acoustically coupled means.	The phrase “or intelligence of any nature” should be stricken from the definition, as it is ambiguous and extremely broad. In the alternative, please clarify what the phrase means.
Telemetry means the automatic recording and transmission of data from remote or inaccessible sources to an information system in a different location for monitoring and analysis. Telemetry data may be relayed using radio, infrared ultrasonic, cellular, satellite or cable, depending on the application.	
(b) *Security incident reporting.* (1)(i) The Contractor shall submit a CISA Incident Reporting Form on all security incidents involving a product or service provided to the Government that includes information and communications technology, or the information system used in ~~developing or~~ providing the product or service, to the Cybersecurity and Infrastructure Security Agency (CISA) in the Department of Homeland Security using the CISA Incident Reporting System. The CISA Incident Reporting System, along with information on types of incidents, can be found here: *https://www.cisa.gov/report.* (ii) Consistent with applicable laws, regulations Governmentwide policies, and Contractor	Reporting mechanism should be harmonized with other reporting mechanisms, such as the one required by DFARS 252.204-7012, to avoid duplicative, confusing and unnecessarily burdensome obligations. The reporting obligation is overly broad to the extent that it includes systems used in developing a product or service. It should be limited to systems directly involved in providing products or services to the government. See proposed revision reflecting this comment. In addition, the government’s permission to share reported information with other agencies should consider the contractor’s policies and contractual obligations, which may impose limitations on

policies and contractual obligations, CISA will share the information reported with any contracting agency potentially affected by the incident, the contractor, or by a vulnerability revealed by the incident and other executive agencies responsible for investigating or remediating cyber incidents, such as the Federal Bureau of Investigation (FBI), and other elements of the intelligence community.	sharing third party information. See proposed revision reflecting this comment. This provision should contain a safe harbor provision that restricts the government from using reported information for certain purposes, *e.g.*, for regulatory investigations, civil litigation, and suspension or debarment.
(2) The Contractor shall also notify the Contracting Officer, and the contracting officer (or ordering officer) of any agency which placed an affected order under this contract, that an incident reporting portal has been submitted to CISA.	In order to align with DFARS 252.204-7012, the rule should not require reporting to the Contracting Officer. If this reporting requirement is included in the final rule, the rule should specify that only limited information should be reported to the Contracting Officer in order to minimize security risks. Specifically, only a CISA incident report number should be provided so that the Contracting Officer can engage CISA for further information.
(3) The Contractor shall thoroughly investigate all relevant indicators that a security incident has occurred and submit information using the CISA incident reporting portal pursuant to paragraphs (b) and (c) of this clause within 8 business hours of confirmation that a security incident has occurred and shall update the submission every 72 business hours thereafter, if there is a material change in the information previously provided, until the Contractor has completed all eradication or remediation activities. Security incidents involving specific types of information (*e.g.*, controlled unclassified information) may require additional reporting that is separate from the requirements of this clause.	The 8hr initial reporting window is unrealistic and should be expanded to 72hrs, which is more realistic and in harmony with the reporting window for DFARS 252.204-7012. The requirement to submit an update every 72hrs is also unduly burdensome and would create a lot of unnecessary submissions. The requirement to submit updates should be contingent upon a material change from the previous update. References to classified information should be removed, as classified information is appropriately addressed by NISPOM. The phrase "may have" should be stricken from this provision because that concept is already captured by the definition of "security incident". See proposed revisions reflecting the above comments.
(4) In the event the Contractor suspects a compromise of its communications or messaging platform, the Contractor should avoid use of such potentially compromised means to provide notification(s) or otherwise communicate information about a security incident and associated response activities.	See proposed revision to clarify scope of contractor obligation.

(c) *Supporting incident response.* (1) *Data preservation and protection.* (i) The Contractor shall collect and preserve for at least 12 months in active storage followed by 6 months in active or cold storage, or until the completion of all remediation and eradication, whichever occurs earlier, available data and information relevant to security incident prevention, detection, response and investigation within information systems used in providing ICT products or services to the Government. For example, this data may include, but is not limited to, network traffic data, full network flow, full packet capture, perimeter defense logs (firewall, intrusion detection systems, intrusion prevention systems), telemetry, and system logs including, but not limited to, system event logs, authentication logs, and audit logs. Upon request by CISA, the Contractor shall promptly provide this data and information to the Government.	This provision suggests that a Contracting Officer is authorized to request preserved data on their own initiative, which they should not be permitted to do. Contracting Officers do not possess the training or expertise to initiate such requests. CISA should be the one requesting this information, not the Contracting Officer. If the Contracting Officer is permitted to request this information from the contractor, the rule should make clear that they may only do so at the direction of CISA, and not on their own initiative. See proposed revision reflecting this comment. If the information is to be provided to the Contracting Officer, a secure means of transmission should be required. The retention period is not industry standard and is unnecessarily costly. We recommend making it the lesser of 12-18 months or completion of remediation/eradication.
(ii) When the Contractor has confirmed that a security incident has occurred on an affected information system, the Contractor shall immediately preserve and protect images of all known affected information systems that impact the federal government's systems and all available monitoring/packet capture data. Following submission of a security incident report pursuant to paragraph (b) of this clause, or receipt of a request for access pursuant to paragraph (c)(6) of this clause, such images and data shall be retained for the longer of— (A) 90 days from the submission of the report or receipt of the request; (B) Any longer period required under paragraph (c)(1)(i) of this clause; or (C) If instructed to retain such images and data beyond 90 days by CISA, until the Contractor is notified by the Contracting Officer that retention is no longer required.	Remove "may", as the definition of security incident already includes the concept of "potential" occurrence. This provision seemingly authorizes the Contracting Officer to order retention of images and data beyond the prescribed window. Such decisions should be made only by CISA, as the Contracting Officer does not possess the qualifications to make such decisions. DFARS 252.204-7012 requires a monitoring window of 90 days, which is industry standard. The 180-day window should be reduced to align with the window in DFARS -7012. See proposed revisions reflecting the above comments.
"(2) *Customization files.* The Contractor shall develop, store, and maintain throughout the life of the contract and for at least 1 year thereafter	Please clarify the scope of what it means for a system to be "used in developing or providing" a service. This phrase is extremely broad and

an up-to-date collection of Contractor-initiated customizations that differ from manufacturer defaults on Contractor-owned devices, computer software, applications, and services, which includes but is not limited to configuration files, logic files and settings on web and cloud applications for all information systems used in providing an ICT product or service to the Government. Upon request by the CISA, or consistent with paragraph (c)(6) of this clause, the Contractor shall provide the cognizant program office/requiring activity, CISA and/or the FBI, with a copy of the current and historical customization files, and notice to CISA that such information has been shared and with whom it has been shared.	ambiguous and could be interpreted to include all of a contractor's information systems with only a tenuous connection to development or performance. This provision seemingly authorizes the Contracting Officer to demand customization files from the contractor. Such decisions should be made only by CISA, as the Contracting Officer does not possess the qualifications to make such decisions. See proposed changes reflecting the above comments.
(3) *Software bill of materials (SBOM).* (i) The Contractor shall maintain, and upon the initial use of such software in the performance of this contract, provide or provide access to the Contracting Officer a current SBOM for each piece of computer software used in performance of the contract. Each SBOM shall be produced in a machine-readable, industry-standard format and shall comply with all of the minimum elements identified in Section IV of The Minimum Elements for a Software Bill of Materials (the current version at the time of solicitation) published by the Department of Commerce at *https://www.ntia.doc.gov/report/2021/minimum-elements-software-bill-materials-sbom*, except for frequency which is addressed in paragraph (c)(3)(ii) of this clause. These minimum elements establish the baseline technology and practices for the provisioning of a SBOM that enable computer software transparency, capturing both the technology and functional operation. (ii) If a piece of computer software used in the performance of the contract is updated with a new build or major release, the contractor must update the computer SBOM in paragraph (c)(3)(i) of this clause to reflect the new version of the computer software and provide (or provide access to) the updated SBOM to the	References to SBOM should be removed in their entirety as outside the scope of the proposed rule. If references to SBOM are retained, the obligation should be limited to first party software the contractor is providing to the government as a deliverable under the contract. As written, the provision has no limitations and may be impossible to comply with. For example, the provision could be interpreted to require SBOMs from third parties for products like Microsoft Word, the operating systems used on computers used in performance, the software on the routers used to connect to the internet, and the software on the wireless earphones used to connect to one's computer. Even if this were reasonable in scope, contractors may not be able to obtain SBOMS from such third parties. The requirement to update SBOMs should not apply to new builds, but just to major version releases. There is no agreed upon definition of "new build," whereas versioning is based on numbering and is clearly defined.

Contracting Officer. This includes computer software builds to integrate an updated component or dependency. (iii) If an SBOM has been provided to the contracting officer at the basic contract level, the SBOM does not need to be provided to the contracting officer for each order.	
(4) *Damage assessment activities*. If the Government elects to conduct a damage assessment regarding a security incident, the Contractor shall promptly provide to the Government, and any independent third party specifically authorized by the Government, all information identified in paragraphs (c)(1), (c)(2), and (c)(3) of this clause.	Use of "the Government" here is ambiguous. Please specify which agencies are authorized to conduct a damage assessment. This provision would seemingly authorize the Contracting Officer to order a damage assessment on their own initiative, which should not be permitted. Any third-party receiving information on behalf of the government needs to be bound by sufficient security and confidentiality requirements. See proposed revisions intended to harmonize with DFARS 252.204-7012.
(5) *Malicious computer software*. If the Contractor discovers and isolates malicious computer software in connection with a security incident, the Contractor shall submit malicious code samples or artifacts to CISA using the appropriate form at *https://www.malware.us-cert.gov* within 8 business hours of discovery and isolation of the malicious computer software in addition to required incident reporting pursuant to paragraph (b) of this clause.	This provision should be harmonized with DFARS 252.204-7012(d) to avoid differing, but functionally duplicative, requirements. Recommend using 8 business hours to ensure contractor has at least one full business day to submit required information. See proposed revision reflecting this comment.
(6) *Access, including access to additional information or equipment necessary for forensic analysis*. (i) Upon request by CISA or the FBI, in response to a security incident reported in accordance with paragraph (b)(1) of this clause, the Contractor shall first validate any CISA or FBI access request according to the procedures in (c)(6)(ii) of this clause, and then respond to any requests for access from the contracting agency, CISA, and the FBI within 96 business hours with available information identified in paragraphs (c)(1), (c)(2), and (c)(3) of this clause.	This provision seemingly authorizes the Contracting Officer to request full access on their own initiative, which they should not be permitted to do. The level of access required by this provision is unprecedented and could create security/privacy risks,and could cause contractors to violate their other contractual obligations relating to privacy and confidentiality. This provision should be scaled back to align with other clauses such as DFARS 252.204-7012, which has been working for years. See proposed revisions reflecting the above comments.

	If the part of this provision requiring access to contractor employees is retained, such access should be limited to the employees with knowledge relevant to the security incident, not all employees involved in the performance of the contract.
(ii) Prior to responding to a request from CISA or the FBI for information or access under this clause, the Contractor shall: (A)(*1*) For requests from CISA, confirm the validity of the request by contacting CISA Central at *report@cisa.gov* or (888) 282–0870, (*2*) For requests from the FBI, confirm the validity of the request by contacting the FBI field office identified by the requestor using contact information from *https://www.fbi.gov/contact-us/field-offices;* and (B) Immediately notify the Contracting Officer and any other agency official designated in the contract in writing of receipt of the request. Provision of information and access to CISA and the FBI under this clause shall not occur until the validity of the request is confirmed by CISA and/or the FBI, as applicable.	This provision underscores prior comments that Contracting Officers should not be permitted to request information or access under this clause, as there is no validation process for such requests. Regarding the last sentence of this provision: Requiring contractor to provide the information before the government responds to a validation request defeats the purpose of having a validation process. Provision of information and access should not occur until the validity of the request is confirmed by CISA and/or the FBI. See proposed revisions reflecting the above comment.
(d) *Cyber threat indicators and defensive measures reporting.* During the performance of the contract, the Contractor is encouraged to either— (1) Subscribe to the Automated Indicator Sharing (AIS) (*https://www.cisa.gov/ais*) capability or successor technology. The Contractor may share cyber threat indicators and recommended defensive measures, to include associated tactics, techniques, and procedures, if available, when such indicators or measures are observed on information and communications technology used in performance of the contract or provided to the Government,	Information sharing should be voluntary (as it always has been), not mandatory. See proposed revisions reflecting the above comment.

in an automated fashion using this medium during the performance of the contract. Contractors submitting cyber threat indicators and defensive measures through AIS will receive applicable legal protections (see 6 U.S.C. 1505) in accordance with the Cybersecurity Information Sharing Act of 2015, Procedures and Guidance; or (2) Participate in an information sharing and analysis organization or information sharing and analysis center with the capability to share indicators with AIS or successor technology and that further shares cyber threat indicators and recommended defensive measures submitted to it with AIS. The Contractor may share cyber threat indicators and recommended defensive measures, when such indicators or measures are observed on information and communications technology used during performance of the contract or provided to the Government, with the ISAO or ISAC during the performance of the contract, in addition to required incident reporting pursuant to paragraph (b) of this clause. Contractors submitting cyber threat indicators and defensive measures through an ISAO or ISAC will receive applicable legal protections in accordance with the Cybersecurity Information Sharing Act of 2015 Procedures and Guidance.	
(e) *Internet Protocol version 6 (IPv6).* (1) This paragraph (e) applies to— (i) Any ICT using internet protocol provided to the Government, and (ii) Any interfaces exposed to the Government from a Contractor information system using internet protocol. (2) The Contractor shall comply with all applicable mandatory capabilities specified in	Exceptions should be made for preexisting contracts that permit pre-IPv6 products.

the current version of the USGv6 Profile (NIST Special Publication 500–267B) (see Office of Management and Budget (OMB) Memorandum M–21–07, Completing the Transition to Internet Protocol Version 6 (IPv6) dated November 19, 2020) and provide to the Contracting Officer a copy of or access to the corresponding supplier's declaration of conformity in accordance with the USGv6 Test Program (see NIST SP 500–281A). (3) The agency may have granted a waiver to this paragraph (e). If so, elsewhere in this contract the waiver will be identified along with any conditions (see FAR 39.106–2).	
(f) *Subcontracts.* The Contractor shall include the substance of this clause, including this paragraph (f), in all subcontracts where ICT is used or provided in the performance of the subcontract, including subcontracts for the acquisition of commercial products or services. All references to the Contractor are applicable to all subcontractors. The Contractor shall require subcontractors to notify the prime Contractor and next higher tier subcontractor within 8 business hours of discovery of a security incident.	Is flowdown required if the prime contract does not involve ICT? Please clarify what it means for ICT to be "used or provided in the performance of the subcontract." As written, the phrase could be interpreted to cover virtually every subcontract. The 8hr reporting window should specify 8 business hours in order to ensure contractors have one full business day to report. See proposed revision reflecting this comment. In connection with subcontracts and flowdown generally, it bears repeating that the Council should consider whether it can: (1) exclude COTS products from full and applicability, (2) exclude subcontractors from flowdown requirements, or (3) consider whether a waiver process is appropriate to ensure access to products or software where compliance is not possible. In addition, we recommend that the Council engage the commercial industrial base to devise a compliance construct whereby the sought compliance with cyber integrity can be achieved in a manner that does not result in placing inordinate, if not near exclusive, risk on the prime contractor.