9110–9B–P

DEPARTMENT OF HOMELAND SECURITY

48 CFR Parts 3001, 3002, 3004, and 3052

[HSAR Case 2015–001; DHS Docket No. DHS–2017–0006]

RIN 1601–AA76

Homeland Security Acquisition Regulation; Safeguarding of Controlled Unclassified Information

AGENCY: Office of the Chief Procurement Officer, Department of Homeland Security (DHS).

ACTION: Final rule.

SUMMARY: DHS is issuing a final rule to amend the Homeland Security Acquisition Regulation (HSAR) to modify a subpart, remove an existing clause and reserve the clause number, update an existing clause, and add two new contract clauses to address requirements for the safeguarding of Controlled Unclassified Information (CUI). This final rule implements security and privacy measures to safeguard CUI and facilitate improved incident reporting to DHS. These measures are necessary because of the urgent need to protect CUI and respond appropriately when DHS contractors experience incidents with DHS information.

DATES: This final rule is effective **[INSERT DATE 30 DAYS AFTER THE DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]**.

FOR FURTHER INFORMATION CONTACT: Shaundra Ford, Procurement Analyst, DHS, Office of the Chief Procurement Officer, Acquisition Policy and Legislation, (202) 447–0056, or email *HSAR@hq.dhs.gov*. When using email, include HSAR Case 2015–001 in the subject line.

SUPPLEMENTARY INFORMATION:

Table of Contents

I. Executive Summary
   A. Purpose of the Regulatory Action
   B. Legal Authority
   C. Costs and Benefits
II. Background
III. Discussion and Analysis
   A. Significant Changes from Proposed Rule
   B. Discussion of Public Comments and Responses
      1. General
      2. Alignment with FISMA, E.O. 13556 (*Controlled Unclassified Information*), and Its Implementing Regulation at 32 CFR Part 2002 (*Controlled Unclassified Information*)
      3. Applicability of NIST SP 800–171
      4. ATO Requirements
      5. CUI Registry
      6. DHS Internal Policies and Procedures
      7. Definitions
      8. Reciprocity in Interagency Regulations and Information Security Requirements
      9. Incident Reporting and Response
      10. Privacy Requirements
      11. Sanitization of Government and Government-Activity-Related Files and Information
      12. Subcontractor Flow-down Requirements
      13. Requirements Applicable to Educational Institutions
      14. Self-deleting Requirements
      15. Applicability to Service Contracts
      16. Costs
IV. Statutory and Regulatory Requirements
   A. Executive Orders 12866 and 13563
      1. Outline of the Analysis
      2. Summary of the Analysis
      3. Subject-by-Subject Analysis
      4. Summary
      5. Regulatory Alternatives
   B. Regulatory Flexibility Act
      1. A statement of the need for, and objectives of, the rule
      2. A statement of the significant issues raised by the public comments in response to the IRFA, a statement of the assessment of the agency of such issues, and a statement of any changes made to the proposed rule as a result of such comments
      3. The response of the agency to any comments filed by the Chief Counsel for Advocacy of the SBA in response to the proposed rule, and a detailed statement of any change made to the proposed rule as a result of the comments
      4. A description of and an estimate of the number of small entities to which the rule will apply or an explanation of why no such estimate is available
      5. A description of the projected reporting, recordkeeping, and other compliance requirements of the rule, including an estimate of the classes of small entities that will be subject to the requirement and the type of professional skills necessary for preparation of the report or record
      6. A description of the steps the agency has taken to minimize the significant economic impact on small entities consistent with the stated objectives of

applicable statutes, including a statement of the factual, policy, and legal reasons for selecting the alternative adopted in the final rule and why each of the other significant alternatives to the rule considered by the agency that affects the impact on small entities was rejected

C. Paperwork Reduction Act

Table of Abbreviations

ATO	Authority to Operate
BAA	Buy American Act
CAGE	Commercial and Government Entity
CIO	Chief Information Officer
COR	Contracting Officer's Representative
CSO	Chief Security Officer
CUI	Controlled Unclassified Information
CVI	chemical-terrorism vulnerability information
DHS	Department of Homeland Security
DoD	Department of Defense
EA	Executive Agent
E.O.	Executive Order
FAR	Federal Acquisition Regulation
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act of 2014
FPDS	Federal Procurement Data System
FR	Federal Register
FRFA	final regulatory flexibility analysis
FTE	full-time equivalent
FY	Fiscal Year
GFE	government-furnished equipment
GSA	General Services Administration
HIPAA	Health Insurance Portability and Accountability Act
HSAR	Homeland Security Acquisition Regulation
IRFA	initial regulatory flexibility analysis
ISAC	Information Sharing and Analysis Center
ISAO	Information Sharing and Analysis Organization
IT	information technology
NAICS	North American Industry Classification System
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
NPRM	notice of proposed rulemaking
OIRA	Office of Information and Regulatory Affairs
OMB	Office of Management and Budget
PCII	protected critical infrastructure information
PII	Personally Identifiable Information
POA&M	Plans of Action and Milestones
POC	Point of Contact
PSC	Product and Service Code
RFA	Regulatory Flexibility Act of 1980, as amended by the Small Business Regulatory Enforcement Fairness Act of 1996
SA	Security Authorization
SBA	Small Business Administration

SME	subject-matter expert
SOC	Security Operations Center
SP	Special Publication
SPII	Sensitive Personally Identifiable Information
SRTM	Security Requirements Traceability Matrix
SSI	Sensitive Security Information
TAA	Trade Agreements Act
TSA	Transportation Security Administration
UEI	Unique Entity Identifier
US-CERT	United States Computer Emergency Readiness Team

I. Executive Summary

A. Purpose of the Regulatory Action

The purpose of this final rule is to implement security and privacy measures to safeguard CUI and facilitate improved incident reporting to DHS. This final rule does not apply to classified information. These measures are necessary because of the urgent need to protect CUI and respond appropriately when DHS contractors experience incidents with DHS information. Persistent and pervasive high-profile breaches of Federal information continue to demonstrate the need to ensure that information security protections are clearly, effectively, and consistently addressed in contracts. This final rule strengthens and expands existing HSAR language to ensure adequate security when: (1) contractor and/or subcontractor employees will have access to CUI; (2) CUI will be collected or maintained on behalf of the agency; or (3) Federal information systems, which include contractor information systems operated on behalf of the agency, are used to collect, process, store, or transmit CUI. Specifically, the final rule:

- Identifies CUI handling requirements and security processes and procedures applicable to Federal information systems, which include contractor information systems operated on behalf of the agency;
- Identifies incident reporting requirements, including timelines and required data elements, inspection provisions, and post-incident activities;

- Requires certification of sanitization of government and government-activity-related files and information; and
- Requires contractors to have in place procedures and the capability to notify and provide credit monitoring services to any individual whose Personally Identifiable Information (PII) or Sensitive PII (SPII) was under the control of the contractor or resided in the information system at the time of the incident.

B. Legal Authority

This rule addresses the safeguarding requirements specified in the Federal Information Security Modernization Act of 2014 (FISMA) (44 U.S.C. 3551, et seq.); Office of Management and Budget (OMB) Circular A–130, *Managing Information as a Strategic Resource*; relevant National Institute of Standards and Technology (NIST) guidance; Executive Order (E.O.) 13556, *Controlled Unclassified Information* (75 FR 68675, Nov. 9, 2010), and its implementing regulation at 32 CFR part 2002; and the following OMB memoranda: M–17–12, *Preparing for and Responding to a Breach of Personally Identifiable Information*; M–14–03, *Enhancing the Security of Federal Information and Information Systems*; and Reporting Instructions for FISMA and Agency Privacy Management as identified in various OMB memoranda.

C. Costs and Benefits

The final rule will apply to DHS contractors that require access to CUI, collect or maintain CUI on behalf of the Government, or operate Federal information systems, which include contractor information systems operating on behalf of the agency, that collect, process, store, or transmit CUI. DHS estimates the final rule will have an annualized cost that ranges from $15.32 million to $17.28 million at a discount rate of 7 percent and a total 10-year cost that ranges from $107.62 million to $121.37 million at a discount rate of 7 percent. The primary contributors to these costs are the independent assessment requirement and reporting and recordkeeping requirements. There are

additional small, quantified costs from rule familiarization and security review processes. DHS was unable to quantify costs associated with incident reporting requirements, PII and SPII notification requirements, credit monitoring requirements and they are therefore discussed qualitatively. DHS was unable to quantify the cost savings or benefits associated with the rule. However, the final rule is expected to produce cost savings by reducing the time required to grant an ATO, reducing DHS time reviewing and reissuing proposals because contractors are better qualified, and reducing the time to identify a data breach. The final rule also produces benefits by better notifying the public when their data are compromised, requiring the provision of credit monitoring services so that the public can better monitor and avoid costly consequences of data breaches, and reducing the severity of incidents through timely incident reporting.

II. Background

DHS published a notice of proposed rulemaking (NPRM) in the *Federal Register* at 82 FR 6429 on January 19, 2017, to implement adequate security and privacy measures to safeguard CUI from unauthorized access and disclosure and facilitate improved incident reporting to DHS. Fourteen respondents submitted public comments in response to the proposed rule. This final rule incorporates the reasoning of the proposed rule except as reflected elsewhere in this preamble.

III. Discussion and Analysis

DHS reviewed the public comments in the development of the final rule. A certain number of the comments received were outside the scope of the rule. A discussion of the comments within the scope of the rule and the changes made to the rule as a result of those comments is provided, as follows:

A. Significant Changes from Proposed Rule

1. HSAR 3052.204-71, *Contractor Employee Access*, is revised as follows:

- Revised paragraph (a) to remove the definition of "sensitive information" and replace it with the definition of "CUI";
- Revised paragraph (b) to remove the definition of "information technology resources" and replace it with the definition of "information resources";
- Replaced all references to "sensitive information" with "CUI" and all references to "information technology resources" with "information resources";
- Revised paragraph (e) to clarify that both initial and refresher training concerning the protection and disclosure of CUI is required;
- Revised paragraph (g) of Alternate I to make clear that additional training on certain CUI categories may be required if identified in the contract; and
- Replaced the reference to "statement of work" in paragraph (h) of Alternate I with "contract."

2. Restructured clause 3052.204-7X, *Safeguarding of Controlled Unclassified Information*, as follows:

- Made the requirements of paragraph (c), *Authority to Operate*, into Alternate I to the basic clause; and
- Made the requirements of paragraphs (f), *PII and SPII Notification Requirements*, and (g), *Credit Monitoring Requirements*, into a separate clause at 3052.204-7Y, *Notification and Credit Monitoring Requirements for Personally Identifiable Information Incidents*. This includes clarifying updates to the *PII and SPII Notification Requirements* section.

3. Revised requirements of restructured clause 3052.204-7X, *Safeguarding of Controlled Unclassified Information*, as follows:

- Made clear that both contractors and subcontractors are responsible for reporting known or suspected incidents to the Department;

- Made clear that subcontractors are required to notify the prime contractor that they have reported a known or suspected incident to the Department;
- Increased the amount of time a vendor must retain monitoring/packet capture data from 90 days to 180 days; and
- Revised the requirements for when prime contractors must include clause 3052.204-7X, *Safeguarding of Controlled Unclassified Information*, in subcontracts.

4. Made clarifying edits to the definitions of the following terms: *Controlled Unclassified Information*, *Sensitive Security Information*, *Homeland Security Agreement Information*, *Information Systems Vulnerability Information*, *Personnel Security Information*, *Privacy Information*, and *Sensitive Personally Identifiable Information*.

5. Made additional amendments to paragraph (b) of clause 3052.212-70 to add clause 3052.204-7Y, *Notification and Credit Monitoring Requirements for Personally Identifiable Information Incidents*.

B. Discussion of Public Comments and Responses

1. General

Comment: Two comments requested that the Department withdraw the proposed rule. One of the comments requested that DHS grant an extension of the comment period if the rule was not going to be withdrawn. The other comment stated that the rule was ill-considered and was not properly coordinated with other agencies that follow and support the principles in 32 CFR part 2002. The comment also stated the rulemaking adds burdens to DHS and its contractors that differ from what is required or expected by others and requested that DHS delay implementation of the entire rule or suspend the

rulemaking process altogether pending further progress with the expected general Federal Acquisition Regulation (FAR) CUI rule.[1]

Response: Given the nature of this rule, and the prevalent and persistent nature of cyber-attacks impacting both public and private networks, DHS declines the respondents' request to withdraw this rule. Failure to proceed with this rule places at risk both the Department's CUI and the information systems where CUI resides, which would be in contravention to the Department's mission and to the public interest. In addition, DHS will neither delay nor suspend this rulemaking pending progress on the FAR CUI rule. A 30-day extension of the comment period from March 20, 2017, to April 19, 2017, was granted. Additionally, DHS conducted extensive interagency coordination while developing this rule, including coordination with NARA. Also, the FAR CUI rule does not eliminate the need for DHS to proceed with this rulemaking. DHS is a participant on the FAR team responsible for drafting the FAR language that will implement the CUI Program and has determined that the issuance of a FAR CUI rule does not eliminate the need for DHS to identify its agency-specific requirements for CUI and the methodology it uses to ensure that Federal information systems, which includes contractor information systems operated on behalf of the agency, that collect, process, store, or transmit CUI are adequately protected. Also, DHS does not agree that this rulemaking adds burdens to DHS and its contractors that differ substantively from what is required or expected by other agencies as the requirements for Federal information systems are largely based in statute, i.e., FISMA (44 U.S.C. 3551, et seq.), and implementing policies promulgated by OMB and NIST. Agency specific requirements such as an independent assessment and security review are not in conflict with these requirements. They are at the discretion of the agency, considered industry best practices, and are actually becoming more pervasive

[1] Rulemaking to implement the National Archives and Records Administration (NARA) CUI program (*see* E.O. 13556 and 32 CFR part 2002).

Governmentwide. Notwithstanding this, DHS has determined that information security is of paramount importance and is prepared to accept the cost impacts stemming from vendor compliance with these requirements.

Comment: One respondent stated that the rule does not clearly articulate how requirements would be applied to professional service providers, what safeguards they would be obligated to provide, or how they would be assessed by DHS.

Response: Clause 3052.204-7X, *Safeguarding of Controlled Unclassified Information*, clearly identifies the requirements applicable to contractors that access or develop CUI under DHS contracts, as well as the information security requirements applicable to Federal information systems, which include contractor information systems operated on behalf of the agency. The applicability of these requirements does not change depending on the type of contractor. As such, there is no need to identify requirements applicable to the subset of contractors that fall within the professional services community.

Comment: One respondent proposed that DHS use a server that requires verification from a higher ranking official so that the information does not enter the wrong hands, such as an extremist group. The respondent also recommended that there should be logins for each official that could be listed on public servers, as long as the server was American, and that citizens trying to access the information should pass a background check to make sure they are not a threat.

Response: The commenter has oversimplified the process by which DHS should ensure CUI is adequately protected, and DHS has made no corresponding changes to the rule. While DHS and its contractors routinely use servers, logins, and passwords to control access on networks and information systems, this is only a subset of the actions required to ensure CUI and the information systems where CUI resides are adequately protected. Making login information publicly available is a violation of information

security policy. Also, limiting servers used by the Department and its contractors to those manufactured only in the United States does not ensure the security of the server and violates statutory requirements that govern Federal procurements. DHS, like other Departments and agencies, adheres to FAR part 25, *Foreign Acquisition*, when purchasing supplies. FAR part 25 details the application of the Buy American Act (BAA) and the Trade Agreements Act (TAA), including the dollar thresholds at which the TAA supersedes the BAA and nondomestic trading partners receive equal treatment with domestic sources. Additionally, the Department already has in place background investigation requirements for Federal employees and contractors that have access to CUI. Where the Department has determined access to CUI must be limited to U.S. citizens and lawful permanent residents, DHS policies and regulations already reflect those requirements.

Comment: One respondent stated that the proposed rule is very important considering how open information is in this day and age, adding that this rule will help secure important information about the U.S. Government.

Response: DHS agrees that this rule is important and that its requirements will help ensure the security of important government information.

Comment: One respondent stated that small businesses should be concerned by this rule, citing that DHS acknowledged that the rule is a "significant" regulatory action that will impact small business. The respondent stated that there is nothing specific in the rule to assure the small business community that it will be able to comply.

Response: This rule is a "significant" regulatory action that will have an impact on small business; however, this comment implies that all small businesses will be impacted equally, which is not the case. Small businesses that routinely provide services to the Government that rely on Federal information systems, which include contractor information systems operated on behalf of an agency, already are positioned to

implement these requirements and always have been required to do so under DHS contracts. Information security and information security requirements applicable to Federal information systems are not based on the size of a particular business but rather on the sensitivity of the information and the impact(s) of unauthorized access to such information. Applying a lesser standard because a business voluntarily operating in this space is considered small would be untenable and in contravention to the mission of the Department. Additionally, it is important to note that DHS's commitment to small business participation is unparalleled, as evidenced by the Department's 12 consecutive ratings of "A" or higher on the Small Business Administration's (SBA) Small Business Procurement Scorecard (*see https://www.sba.gov/document/support-department-homeland-security-contracting-scorecard*). The Department expressed in the proposed rule its interest in receiving comments from small business concerns related to this rule and has thoroughly considered and adjudicated all comments received.

Comment: One respondent stated that guidance on DHS CUI requirements for cleared facilities should be consistent with Department of Defense (DoD) cleared facility requirements.

Response: The protection of classified information at contractor locations, whether cleared by DoD or another government agency, is outside the scope of this regulation. CUI is protected according to the underlying law, regulation, or Governmentwide policy. DHS does not have the broad authority to waive CUI safeguarding or dissemination requirements that differ from those of classified information.

Comment: One respondent questioned if the proposed rule covers sharing of information on software vulnerabilities with Information Sharing and Analysis Organizations (ISAOs) or Information Sharing and Analysis Centers (ISACs). The respondent also questioned if the ISAOs or ISACs require flow-down of the clauses to

ensure that their members provide adequate protection in accordance with the DHS proposed rule. The respondent stated such a requirement would impose a significant barrier for private sector entities to participate in information sharing.

Response: DHS shares information with ISAOs and ISACs through information sharing agreements between the Government and the ISAO/ISAC, not through contracts. Generally, information sharing agreements do not include the clauses.

2. Alignment with FISMA, E.O. 13556 (*Controlled Unclassified Information*), and Its Implementing Regulation at 32 CFR Part 2002 (*Controlled Unclassified Information*)

Comment: Several respondents stated that the proposed rule is not consistent with FISMA, E.O. 13356, and 32 CFR part 2002.

Response: (a) Alignment with FISMA: The rule is fully consistent with FISMA. FISMA and its predecessor, the Federal Information Security Management Act of 2002, require that agency heads provide "information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—(i) information collected or maintained by or on behalf of the agency; and (ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency . . . ." *See*, *e.g.*, 44 U.S.C. 3554(a)(1)(A). The rule is consistent with these requirements by requiring that information collected or maintained on behalf of the Department and information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency are adequately protected. The rule does this in two ways by identifying: (1) requirements and DHS policies and procedures for handling and protecting CUI collected and maintained on behalf of the Department; and (2) security requirements and procedures for information systems used or operated by a contractor on behalf of an agency.

(b) Alignment with E.O. 13556 and 32 CFR part 2002: The rule is fully consistent with E.O. 13556 and 32 CFR part 2002 (81 FR 63324, Sept. 14, 2016). The NARA CUI rule requires Departments and agencies to develop internal policies and procedures to implement the requirements of the CUI Program.[2] These policies and procedures are subject to review and approval by the CUI Executive Agent (EA) before they are finalized. In addition, the NARA CUI rule establishes baseline information security requirements necessary to protect CUI Basic[3] on nonfederal information systems by mandating the use of NIST Special Publication (SP) 800–171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*, when establishing security requirements to protect CUI's confidentiality on nonfederal information systems. However, consistent with 32 CFR 2002.14(a)(3) and (g), "[a]gencies may increase CUI Basic's confidentiality impact level above moderate only internally, or by means of agreements with agencies or non-executive branch entities (including agreements for the operation of an information system on behalf of the agencies)." Relatedly, 32 CFR 2002.4(c) states that agreements "include, but are not limited to, contracts, grants, licenses, certificates, memoranda of agreement/arrangement or understanding, and information-sharing agreements or arrangements." Therefore, DHS can require a confidentiality impact level above moderate through agreements with non-

---

[2] The NARA CUI rule is implemented at 32 CFR part 2002 (81 FR 63324). That regulation describes the executive branch's CUI Program and establishes policy for designating, handling, and decontrolling information that qualifies as CUI. The CUI Program standardizes the way the executive branch handles information that requires protection under laws, regulations, or Governmentwide policies but that does not qualify as classified under E.O. 13526, *Classified National Security Information* (Dec. 29, 2009), or any predecessor or successor order, or the Atomic Energy Act of 1954 (42 U.S.C. 2011, et seq.), as amended.

[3] *CUI Basic* is the subset of CUI for which the authorizing law, regulation, or Governmentwide policy does not set out specific handling or dissemination controls. Agencies handle CUI Basic according to the uniform set of controls set forth in 32 CFR part 2002 and the CUI Registry. CUI Basic controls apply whenever CUI Specified ones do not cover the involved CUI. *CUI Specified* is the subset of CUI in which the authorizing law, regulation, or Governmentwide policy contains specific handling controls that it requires or permits agencies to use that differ from those for CUI Basic. The CUI Registry indicates which laws, regulations, and Governmentwide policies include such specific requirements. CUI Specified controls may be more stringent than, or may simply differ from, those required by CUI Basic; the distinction is that the underlying authority spells out specific controls for CUI Specified information and does not for CUI Basic information. CUI Basic controls apply to those aspects of CUI Specified where the authorizing laws, regulations, and Governmentwide policies do not provide specific guidance.

executive branch entities. Nonetheless, the information system security requirements of this rule are focused on those applicable to Federal information systems.

Comment: One respondent stated that the revisions to the HSAR must be coordinated as part of the DHS implementation of the CUI Program, per the milestones established by CUI Notice 2016–01, *Implementation Guidance for the Controlled Unclassified Information Program*.

Response: CUI Notice 2016–01, *Implementation Guidance for the Controlled Unclassified Information Program*, was superseded by CUI Notice 2020–01, *CUI Program Implementation Guidelines*, issued May 14, 2020. Neither of the CUI Notices provide guidance on coordination of rulemakings. Nonetheless, DHS conducted extensive interagency coordination while developing this rule, including coordination with NARA.

Comment: One respondent stated that the proposed rule federalizes contractor systems that are not used in an operational capacity on behalf of the Government.

Response: The rule does not federalize contractor systems that are not used in an operational capacity on behalf of the Government. Conversely, it recognizes that there are circumstances when contractor information systems are operated on behalf of an agency. When this is the case, the contractor information system is considered a Federal information system and is subject to the same information system security requirements required for Federal information systems. The rule identifies the security requirements and processes such systems must meet before they are able to operate on behalf of the agency. These requirements are now provided as Alternate I to the basic clause. The rulemaking does not identify any information system security requirements or processes for information systems that are not categorized as Federal information systems. The applicability of the basic clause is not predicated on the type of information system, i.e., Federal or nonfederal. The basic clause is limited to definitions, DHS CUI handling

requirements, incident reporting and response requirements, and sanitization requirements. These requirements exist whenever CUI will be accessed or developed under a contract regardless of the type of information system involved in contract performance. This is the reason why the basic clause is more broadly applicable. DHS was intentionally silent in this rule on the requirements applicable to nonfederal information systems as that was never the purpose of this rulemaking, and the FAR CUI rule is intended to address the requirements for these information systems.

Comment: One respondent requested that DHS revise the scope of its rule to clarify or remove the language related to accessing CUI.

Response: Contractors and subcontractors that have access to CUI are responsible for ensuring the information is handled and safeguarded appropriately and reporting any known or suspected incidents regarding the information for which they have access. As such, DHS declines to revise the scope of the rule to clarify or remove language related to accessing CUI.

Comment: One respondent expressed concern that clause 3004.470-3 requires that "CUI be safeguarded wherever such information resides," including on both "contractor-owned and/or operated information systems operating on behalf of the agency" as well as "any situation where contractor and/or subcontractor employees may have access to CUI." The respondent also expressed concern that contracting officers are required to insert clause 3052.204-7X, *Safeguarding of Controlled Unclassified Information*, in all solicitations and contracts where contractor and/or subcontractor employees will have access to CUI and that the clause requires contractors provide "adequate security to protect CUI," which "includes compliance with DHS policies and procedures in effect at the time of contract award. These policies and procedures are accessible at *https://www.dhs.gov/dhs-security-and-training-requirements-contractors*." Another

respondent similarly stated that inclusion of these statements improperly subjects all contractors and all contractor information systems to DHS agency-specific standards.

Response: Some of the policies and procedures currently posted to the DHS publicly facing website predate the CUI E.O. and the NARA CUI rule. DHS, like many other Departments and agencies, is still in the process of implementing the CUI Program. This process includes an update to internal policies and procedures related to CUI. Once these policies and procedures have been drafted and finalized, they will replace the policies and procedures currently listed on the publicly facing website. These policies and procedures are required to address all elements of the CUI Program and extend beyond the protection of CUI in information systems. For example, the new policies and procedures also will address training, handling, transmission, marking requirements, incident reporting, etc. The current DHS-specific policies and procedures on the publicly facing website address these requirements and the new policies and procedures will as well. As such, compliance with these policies and procedures is mandatory.

It appears that the respondents have focused on the information system security policies that are incorporated into the rule without also considering the other policies and procedures identified, all of which have varying applicability depending on the specifics of the contract. For example, one of the policies referenced governs the Department's background investigation process and security requirements applicable to individuals who have access to the Department's sensitive but unclassified information, now known as CUI. It is both necessary and appropriate that DHS mandate that its contractors comply with these requirements. Anything less is inconsistent with the mission of the Department, has the potential to place important government information at risk, and is contrary to the public interest. Like many of the other DHS policies referenced, the need to comply with this requirement is based on access to the information, not whether a Federal information system or nonfederal information system will process, store, or

transmit the data. Also, the applicability of the information system security policies is specifically defined in the text of clause 3052.204-7X, *Safeguarding of Controlled Unclassified Information*. Specifically, Alternate I, *Authority to Operate*, documents the applicability of *DHS Sensitive Systems Policy Directive 4300A* and *DHS 4300A Sensitive Systems Handbook*. The prescription for Alternate I is clear that these requirements are applicable when Federal information systems, which include contractor information systems operated on behalf of the agency, are used to collect, process, store, or transmit CUI. In addition, the first sentence of proposed paragraph (c), *Authority to Operate*, of clause 3052.204-7X, *Safeguarding of Controlled Unclassified Information*, specifically stated that its requirements are "applicable only to Federal information systems, which include[] contractor information systems operating on behalf of the agency." As such, it is clear that it is not the intent of the Department to levy the requirements in these policies and procedures on contractor information systems that are not operated on its behalf. Lastly, the basic clause is limited to definitions, DHS CUI handling requirements, incident reporting and response requirements, and sanitization requirements. These requirements exist whenever CUI will be accessed or developed under a contract regardless of the type of information system involved in contract performance. This is the reason why the basic clause is more broadly applicable.

Also, the statements in paragraph (a) of clause 3004.470-3, *Policy*, are levied on DHS contractors through the inclusion of clause 3052.204-7X, *Safeguarding of Controlled Unclassified Information*, in the solicitation and resultant contract. Absent inclusion of the clause in the contract, the requirements are not applicable.

Comment: One respondent stated that the proposed rule fails to reflect the information systems safeguarding requirements of the CUI Federal regulation (32 CFR part 2002) and allows DHS full discretion on what electronic safeguarding controls to apply to contractors for any category of CUI. The respondent asserted that the rule makes

no distinction operationally in the way nonfederal contractor information systems and DHS agency information systems are treated, a distinction made in the CUI regulation (32 CFR part 2002) and in FISMA.

Response: The respondent is incorrect that the rule: (1) allows DHS full discretion on what electronic safeguarding controls to apply to contractors for any category of CUI; and (2) makes no distinction between nonfederal contractor information systems and the Federal information systems. DHS understands that the information security requirements applicable to Federal information systems differ from the requirements applicable to nonfederal information systems, as referenced in footnote 5 of the proposed rule, which advised that DHS is aware NIST Special Publication 800–171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations, was released in June 2015 to provide federal agencies with recommended requirements for protecting the confidentiality of Controlled Unclassified Information on non-Federal information systems. However, the information system security requirements in this proposed rulemaking are focused on Federal information systems, which include contractor information systems operating on behalf of an agency, and consistent with 32 CFR part 2002, these information systems are not subject to the requirements of NIST Special Publication 800–171.

DHS also makes this distinction in the prescription for Alternate I, *Authority to Operate*, to clause 3052.204-7X, *Safeguarding of Controlled Unclassified Information*. It specifies that these requirements are applicable when Federal information systems, which include contractor information systems operated on behalf of the agency, are used to collect, process, store, or transmit CUI. Additionally, the first sentence of paragraph (c), *Authority to Operate*, of clause 3052.204-7X, *Safeguarding of Controlled Unclassified Information*, in the proposed rule stated "[t]his subsection is applicable only to Federal information systems, which include[] contractor information systems operating on behalf

of the agency." As such, the Department has made clear it understands there are differing requirements for nonfederal information systems and has not, through the rule, retained full discretion on what electronic safeguarding controls to apply to contractors for any category of CUI.

Comment: One respondent expressed concerns regarding clause 3004.470-4(a), which states "subcontractor employee access to CUI or government facilities must be limited to U.S. citizens and lawful permanent residents." The respondent stated that this limitation is not a legal requirement and recommended that access to government facilities be treated as a separate and distinct issue from the issue of access to CUI and that access limitations for CUI be based on the associated legal requirement as outlined in the NARA CUI rule.

Response: This recommendation is outside the scope of this regulation. DHS notes that although CUI Basic does not inherently convey citizenship or residency requirements, some of the limited dissemination caveats that can be appended to CUI Basic do. While 32 CFR part 2002 does standardize the safeguarding and dissemination requirements that can be imposed on those with whom CUI is shared, the determination and decision to share CUI information remains subject to agency policy and discretion.

3. Applicability of NIST SP 800–171

Comment: Several respondents raised concerns regarding the applicability of NIST SP 800–171. Some of the respondents correctly recognized that the information system security requirements in the proposed rule are specific to Federal information systems, which include contractor information systems operated on behalf of the Government. These respondents expressed concern that the rule did not address the information system security requirements applicable to nonfederal information systems and requested that DHS identify the information system security requirements applicable to nonfederal information systems either through this rulemaking or another one.

Response: DHS does not accept the suggestion to identify the information system security requirements applicable to nonfederal information systems. The rule is intentionally silent on the security requirements applicable to nonfederal information systems because NARA is working with the FAR Councils, in which DHS is a participant, to develop a FAR CUI rule that addresses the requirements nonfederal information systems must meet before processing, storing, or transmitting CUI. As such, there is no need for the Department to identify requirements applicable to nonfederal information systems in this rulemaking, as inclusion would be duplicative and redundant to the work of the FAR Councils.

Comment: Several respondents did not recognize that the scope of the information system security requirements in the proposed rule were specific to Federal information systems and believed that the Department either conflated the two different categories of information systems (i.e., Federal and nonfederal) or was incorrectly applying requirements for Federal information systems to nonfederal information systems (i.e., contractor information systems that are not operated on behalf of the Department). These respondents either requested that DHS refine the scope of the rule to exclude contractor information systems or explicitly identify NIST SP 800–171 as the applicable security standard for contractor information systems. One respondent stated that the proposed rule requires contracting officers to insert proposed clause 305.204-7X, *Safeguarding of Controlled Unclassified Information*, too often (i.e., any time the contractor or subcontractor will have access to CUI regardless of the type of information system being used).

Response: DHS does not accept the recommendation to modify the scope of the rule to exclude contractor information systems or explicitly identify NIST SP 800–171 as the applicable security standard for such systems. There is a misconception among industry actors that NIST SP 800–171 is the only policy that must be followed when CUI

is provided or accessed under a contract. This is not correct. As discussed in the preamble of the proposed rule, OMB Circular A–130, *Managing Information as a Strategic Resource*, makes clear that a contractor information system can be considered a Federal information system if it operates on behalf of an agency. Specifically, Circular A–130 defines a Federal information system as an information system used or operated by an agency or by a contractor of an agency or by another organization on behalf of an agency. In accordance with FISMA, Departments and agencies are responsible for determining when a contractor information system is operated on its behalf. As such, a blanket exclusion of contractor information systems absent a determination of the type of system (i.e., Federal or nonfederal) is not appropriate.

When the Government determines that a contractor information system is being operated on its behalf, that information system is considered a Federal information system and subject to the requirements of NIST SP 800–53, *Security and Privacy Controls for Information Systems and Organizations*. Alternatively, NIST SP 800–171 is applicable "(1) when the CUI is resident in a nonfederal system and organization; (2) when the nonfederal organization is *not* collecting or maintaining information on behalf of a federal agency or using or operating a system on behalf of an agency; and (3) where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or governmentwide policy for the CUI category listed in the CUI Registry" (emphasis original; footnote omitted).

Generally speaking, should the Government determine that a contractor information system is not operated on its behalf, NIST SP 800–171 is applicable. However, consistent with 32 CFR 2002.14(a)(3) and (g), "[a]gencies may increase CUI Basic's confidentiality impact level above moderate only internally, or by means of agreements with agencies or non-executive branch entities (including agreements for the operation of an information system on behalf of the agencies)." Relatedly, 32 CFR

2002.4(c) states that agreements "include, but are not limited to, contracts, grants, licenses, certificates, memoranda of agreement/arrangement or understanding, and information-sharing agreements or arrangements." Therefore, Departments and agencies can require a confidentiality impact level above moderate for nonfederal information systems through agreements with non-executive branch entities. Nonetheless, the information system security requirements of this rule, including those in *DHS Sensitive Systems Policy Directive 4300A* and *DHS 4300A Sensitive Systems Handbook*, are specific to Federal information systems.

As stated in the preamble of the proposed rule, the Government believed that requirements of proposed clause 3052.204-7X, *Safeguarding of Controlled Unclassified Information*, were written in such a way that they would be self-deleting when they are not applicable to a solicitation or contract. For example, the first sentence of paragraph (c), *Authority to Operate*, of the proposed clause stated "[t]his subsection is applicable only to Federal information systems, which include[] contractor information systems operating on behalf of the agency." This section of the clause also defined the applicability of *DHS Sensitive Systems Policy Directive 4300A* and *DHS 4300A Sensitive Systems Handbook*, making clear these policies are applicable only to Federal information systems. Additional examples include language for the notification and credit monitoring requirements stating that the applicability is limited to incidents involving PII or SPII. The remaining requirements of the proposed clause did not include any caveats on their applicability because compliance with them is mandatory regardless of the type of information system (i.e., Federal information system or nonfederal information system).

However, DHS believes the concerns raised regarding proper understanding of the applicability of the requirements of proposed clause 3052.204-7X, *Safeguarding of Controlled Unclassified Information*, are legitimate. In response, DHS has: (1) made the

requirements of paragraph (c), *Authority to Operate*, Alternate I to the basic clause 3052.204-7X, *Safeguarding of Controlled Unclassified Information*; and (2) made the requirements of paragraphs (f), *PII and SPII Notification Requirements*, and (g), *Credit Monitoring Requirements*, a separate clause at 3052.204-7Y titled *Notification and Credit Monitoring Requirements for Personally Identifiable Information Incidents*. As a result of these changes, basic clause 3052.204-7X, *Safeguarding of Controlled Unclassified Information*, is limited to the following provisions: paragraphs (a), *Definitions*; (b), *Handling of Controlled Unclassified Information*; (c), *Incident Reporting Requirements*; (d), *Incident Response Requirements*; (e), *Certification of Sanitization of Government and Government-Activity-Related Files and Information*; (f), *Other Reporting Requirements*; and (g), *Subcontracts*. Compliance with these requirements is mandatory regardless of the information system type (i.e., Federal information system or nonfederal information system). Alternate I to the basic clause is applicable when Federal information systems, which include contractor information systems operated on behalf of the agency, are used to collect, process, store, or transmit CUI. New clause 3052.204-7Y, *Notification and Credit Monitoring Requirements for Personally Identifiable Information Incidents*, is applicable to solicitations and contracts where a contractor will have access to PII. These changes were made to: (1) ensure that DHS contractors clearly understand the scope and applicability of the various requirements contained in proposed clause 3052.204-7X, *Safeguarding of Controlled Unclassified Information*; (2) make clear that the Authority to Operate (ATO) requirements of the clause are only applicable to Federal information systems, which include contractor information systems operated on behalf of the agency; and (3) ensure that DHS contractors understand credit monitoring and notification requirements are only applicable when the solicitation and contract require contractor access to PII.

Comment: Several respondents raised concerns about footnote 5 in the proposed rule. The footnote advised that DHS is aware NIST Special Publication 800–171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations, was released in June 2015 to provide federal agencies with recommended requirements for protecting the confidentiality of Controlled Unclassified Information on non-Federal information systems. However, the information system security requirements in this proposed rulemaking are focused on Federal information systems, which include contractor information systems operating on behalf of an agency, and consistent with 32 CFR part 2002, these information systems are not subject to the requirements of NIST Special Publication 800–171.

One respondent interpreted the footnote to mean that DHS believes NIST SP 800–171 is applicable to nonfederal entities that handle, process, use, share, or receive CUI. One respondent raised concerns that the proposed rule was not consistent with the footnote because the rule requires in clause 3004.470-3(a) that CUI be safeguarded in "any situation where contractor and/or subcontractor employees may have access to CUI." Another respondent stated that the footnote downplays the applicability of NIST SP 800–171 and implies that the guidance is for the more limited set of systems covered by NIST SP 800–53. The same respondent advised that in other parts of the rule, contractors' internal business systems that do fall under the provisions of NIST SP 800–171 are specifically called out. Specific actions requested include:

- Moving the content of footnote 5 to the *Background* section to improve the clarity of the scope of the rule and avoid unnecessary misinterpretations and misunderstandings;
- Making clear that the proposed rule does not apply to contractor information systems;

- Clarifying that the "adequate security" requirements of the rule do not apply to internal contractor information systems that are not operated on behalf of an agency, and stressing that the use of sanitization procedures for CUI spills onto internal contractor information systems, instead of requiring "adequate security" implementation on systems "regardless of where" the CUI may reside; and
- Clarifying that contractors are not responsible for implementing the "adequate security" requirements on government-furnished equipment (GFE) that contractors operate in their own internal contractor environment, unless specifically agreed between the DHS procuring activity (i.e., contracting office) and the contractor.

Response: There appears to be a misunderstanding within industry regarding the applicability of NIST SP 800–171. Categorization as a nonfederal entity does not mean the security requirements for information systems used by a nonfederal entity default to those provided for in NIST SP 800–171. The Government must first determine if the contactor information system is operated on its behalf, thus making the information a Federal information system. If the Government determines the contractor information system is operated on its behalf, then the system is required to comply with NIST SP 800–53. Generally speaking, if the Government determines that the contractor information system is not operated on its behalf, NIST SP 800–171 is applicable. The Government's determination of the type of system, Federal versus nonfederal, must be made before any decision can be made on the security requirements applicable to the information system.

Commenters are incorrect in stating that the proposed rule is not consistent with the footnote by requiring that CUI be safeguarded in "any situation where contractor and/or subcontractor employees may have access to CUI." CUI is required to be handled properly and adequately safeguarded at all times. As previously stated, it appears that the

respondents have focused on the information system security policies that are incorporated into the rule with no regard for the other policies and procedures identified, all of which have varying applicability depending on the specifics of the contract. The only requirement in proposed clause 3052.204-7X, *Safeguarding of Controlled Unclassified Information*, applicable to information systems was paragraph (c), *Authority to Operate*. The remaining requirements of the proposed clause, namely paragraphs (b), *Handling of Controlled Unclassified Information*, (d), *Incident Reporting Requirements*, (e), *Incident Response Requirements*, (f), *PII and SPII Notification Requirements*, (g), *Credit Monitoring Requirements*, (h), *Certificate of Sanitization of Government and Government-Activity-Related Files and Information*, (i), *Other Reporting Requirements*, and (j), *Subcontracts*, are applicable regardless of the type of information system (i.e., Federal or nonfederal), as well as when information systems are not used and only paper documents are available under the contract. *DHS Sensitive Systems Policy Directive 4300A* and *DHS 4300A Sensitive Systems Handbook* are only applicable to Federal information systems. The prescription for Alternate I is clear that the ATO requirements are applicable only when Federal information systems, which include contractor information systems operated on behalf of the agency, are used to collect, process, store, or transmit CUI. Additionally, the proposed rule made clear this point by specifically stating in the first sentence of paragraph (c), *Authority to Operate*, of clause 3052.204-7X, *Safeguarding of Controlled Unclassified Information*, that the "subsection is applicable only to Federal information systems, which include[] contractor information systems operating on behalf of the agency."

The footnote is no longer included in the rule and DHS has provided significant information regarding the applicability of NIST SP 800–171 throughout the *Discussion and Analysis* section of the rule. These statements not only address the applicability of the publication to nonfederal information systems, but they also address the ability of

Departments and agencies to increase CUI Basic's confidentiality impact level above moderate on nonfederal systems (i.e., beyond the requirements of NIST SP 800–171), pursuant to the terms of an agreement as provided for in 32 CFR part 2002.

DHS declines the recommendation to clarify that the rule is not applicable to contractor information systems. As previously stated, the only requirement in the proposed rule specific to information systems was paragraph (c), *Authority to Operate*, in clause 3052.204-7X, *Safeguarding of Controlled Unclassified Information*; in this final rule, the requirements of that paragraph have been made into Alternate I to the basic clause. All the other requirements are applicable regardless of the type of information system (i.e., Federal or nonfederal), as well as when information systems are not used, making the requirements applicable to contractors that access or develop CUI under DHS contracts. Also, absent a determination of the status of the contractor information system as Federal or nonfederal, it would be inappropriate for DHS to state that the rule is not applicable to contractor information systems.

DHS declines the recommendation to clarify that the "adequate security" requirements of the rule do not apply to internal contractor information systems that are not operated on behalf of an agency, and stress that the use of sanitization procedures for CUI spills onto internal contractor information systems, instead of requiring "adequate security" implementation on systems "regardless of where" the CUI may reside. The requirement for adequate security is not solely specific to information systems. Adequate security includes ensuring security protections are applied commensurate with the risk resulting from unauthorized access, use, disclosure, disruption, modification or destruction of the information. It also includes ensuring information contractors and subcontractors host on information systems on behalf of the agency, as well as information systems and applications used by the agency, operate effectively and provide appropriate protections related to confidentiality, integrity, and availability.

Additionally, paragraph (b)(1) of clause 305.204-7X, *Safeguarding of Controlled Unclassified Information*, requires contractors and subcontractors to provide adequate security to protect CUI from unauthorized access and disclosure. This includes complying with DHS policies and procedures, accessible at *https://www.dhs.gov/dhs-security-and-training-requirements-contractors*, in effect when the contract is awarded.

A review of the policies and procedures on the referenced website would demonstrate that the applicability of the various policies and procedures depends on the requirements of each contract, including the type(s) of CUI accessed or developed under the contract. In addition, the clause makes clear that the information system security policies and procedures on the website are only applicable to Federal information systems. Also, the respondent is incorrect that internal contractor information systems that are not operated on behalf of the agency should not be required to have adequate security. If such a system includes the Department's CUI, it is imperative that adequate security of the system be maintained. Nonetheless, the information system security requirements of this rule are limited to Federal information systems. The purpose of this rule is the safeguarding of CUI, so it would be inappropriate to assert that DHS was attempting to apply security standards to contractor information systems that do not contain CUI. Also, "CUI spills onto internal contractor information systems" are considered incidents and are subject to the incident reporting and response requirements of clause 3052.204-7X, *Safeguarding of Controlled Unclassified Information*.

DHS declines the recommendation to clarify that contractors are not responsible for implementing the "adequate security" requirements on GFE that contractors operate in their own internal contractor environment, unless specifically agreed between the DHS procuring activity and the contractor. Clause 3052.204-7X *Safeguarding of Controlled Unclassified Information*, is clear on the applicability of the information system security

requirements and, as such, there is no need to state within the text of the clause that the requirements are not applicable to GFE.

4. ATO Requirements

Comment: One respondent stated that it appears as if the requirements of paragraph (c)(1)(i) of proposed clause 3052.204-7X, *Safeguarding of Controlled Unclassified Information*, would apply only to an information system that is in development and the security authorization (SA) package must be submitted before the system goes operational.

Response: The respondent is partially correct. The SA package must be submitted and ATO granted before a Federal information system, which includes a contractor information system operated on behalf of the agency, can be used to collect, process, store, or transmit CUI. However, the requirement for submission of a SA package is not limited to information systems that are under development. Whether the Federal information system is under development or already in existence, before it can be used to collect, process, store, or transmit CUI it must receive an ATO from DHS and the requirements for submission of the SA package must be met.

Comment: The same respondent questioned if the ATO requirements are applicable to nonfederal information systems. If so, the respondent stated that the clause should state when the SA package for these systems must be submitted as well as clarify the applicability of the independent assessment and which standard (i.e., NIST SP 800–53 or NIST SP 800–171) will be used to determine compliance.

Response: The prescription for Alternate I identifies that these requirements are applicable when Federal information systems, which include contractor information systems operated on behalf of the agency, are used to collect, process, store, or transmit CUI. Additionally, the first sentence of paragraph (c), *Authority to Operate*, in proposed clause 3052.204-7X, *Safeguarding Controlled Unclassified Information*, stated "[t]his

subsection is applicable only to Federal information systems, which include[] contractor information systems operating on behalf of the agency." As such, the information system security requirements of the clause are applicable only to Federal information systems. As previously stated, DHS is intentionally silent on the requirements applicable to nonfederal information systems as the FAR CUI rule is intended to address the requirements for these information systems. Inclusion of such requirements in this rule would be duplicative and redundant to the work of the FAR Councils.

Comment: One respondent stated that the proposed clause could be interpreted to require that contractors meet the security requirements of NIST SP 800–53 when safeguarding CUI at DHS prior to collecting, processing, storing, or transmitting CUI. The respondent also stated that a contractor will need to have gone through the DHS ATO process and demonstrated its capabilities to meet the requirements of the proposed clause. The respondent raised concerns that such a process thwarts the "do once, use many" efficiencies established under the Federal Risk and Authorization Management Program (FedRAMP). Additionally, the respondent stated that absent definitive guidance on the timing of the ATO, unnecessary expenses may be incurred by potential offerors, or competition may be needlessly stifled, precluding access to best commercial solutions and innovative new technology.

Response: Consistent with FISMA and its implementing Governmentwide policies, Federal information systems, which include contractor information systems operated on behalf of the Government, are required to receive an ATO before they can collect, process, store, or transmit Federal information. This requirement does not mean that a contractor's information system must have received an ATO from the Department before a contractor responds to a DHS solicitation. To require a contractor to obtain an ATO before contract award is costly and unnecessarily burdensome, and it could potentially place contractors in the position to incur costs that they would have no

possibility to recoup. Clause 3052.204-7X, *Safeguarding of Controlled Unclassified Information*, documents the timeline and process contractors must comply with to receive an ATO from the Department and it is clear that this process takes place after a contract award is made.

Comment: One respondent asserted that DHS should tie new regulatory requirements on cybersecurity controls to FedRAMP. Another respondent stated that the rule does not recognize or accommodate the use of cloud services.

Response: FedRAMP addresses requirements for cloud computing. To the extent a contractor is proposing a cloud solution to the Department, DHS would comply with FedRAMP policies and procedures. This includes the expectation that contractors would rely on the documents the cloud service provider used to obtain its provisional ATO under FedRAMP and modify them to reflect any additional requirements necessary to provide the specific services required by the Department.

Comment: One respondent stated that the proposed process will impose significant responsibilities on DHS, will require a great expense to the contractor, and will end up limiting competition.

Response: DHS recognizes there are significant costs associated with these requirements; however, the persistent and prevalent nature of cyber-attacks on both government and private sector networks has shown that this is a necessary expense. DHS fully expects its contractors to reflect these costs in the price and cost proposals they submit to the Department.

Comment: Two respondents raised concerns regarding the applicability of the rule to contracts awarded using the procedures of FAR part 12, *Acquisition of Commercial Items.* The respondents stated that applying the requirements of the rule to contracts awarded under the procedures of this FAR part impact the Department's access to innovative technology and increase the number of obstacles to market entry to the DHS

supply chain for these companies as well as new start-ups with innovative technical ideas. The respondents recommended that DHS exclude commercial items from the requirements of the rule.

Response: DHS relies extensively on commercial contractors to provide services that include access to and the processing, storing, and transmitting of CUI. Eliminating this large pool of contractors from compliance with these requirements is untenable. It is not only inconsistent with the mission of the Department, but it is also contrary to the public interest. DHS has determined that the costs associated with compliance with the security requirements of this rule are a necessary expense to ensure DHS CUI is adequately protected.

Comment: One respondent recommended that DHS specify if the Department will be the arbiter of compliance or if contractor self-assessments will suffice, the latter of which is the preference of the respondent.

Response: Clause 3052.204-7X, *Safeguarding of Controlled Unclassified Information*, is clear that a contractor operating a Federal information system, which includes a contractor information system operated on behalf of the agency, must receive an independent assessment. Specifically, the clause requires contractors have an independent third party validate the security and privacy controls in place for the information system(s). Validation includes reviewing and analyzing the SA package and reporting on technical, operational and other deficiencies as outlined in NIST Special Publication 800-53, Security and Privacy Controls for Information Systems and Organizations. Deficiencies must be addressed before the SA package is submitted to the COR for review. DHS will review the independent assessment and, in conjunction with its own analysis, determine if an ATO should be granted.

Comment: One respondent recommended if DHS will be responsible for determining if a contractor has implemented adequate security that the rule clarify how

any determination of adequacy will be made. The respondent requested that the authority be placed at a level higher than the contracting officer, such as the Chief Information Officer (CIO), to ensure a more uniform application across DHS. The respondent also recommended that DHS include further guidance on this subject on the cited website to explain to contractors how this standard will be applied.

Response: Clause 3052.204-7X, *Safeguarding of Controlled Unclassified Information*, consistently has identified that the Component or Headquarters CIO, or designee, is responsible. Alternate I, which incorporates paragraph (c) of the proposed clause, states that "[t]he Contractor shall not collect, process, store, or transmit CUI within a Federal information system until an ATO has been granted by the Component or Headquarters CIO, or designee." Alternate I makes clear that these requirements are only applicable to Federal information systems and the Component or Headquarters CIO, or designee, is responsible for determining if a contractor has implemented adequate security.

DHS declines the recommendation to add further guidance on this topic on the publicly facing website. Adequate security means ensuring security protections are applied commensurate with the risk resulting from unauthorized access, use, disclosure, disruption, modification or destruction of the information. It also includes ensuring information contractors and subcontractors host on information systems on behalf of the agency, as well as information systems and applications used by the agency, operate effectively and provide appropriate protections related to confidentiality, integrity, and availability.

Additionally, paragraph (b)(1) of clause 3052.204-7X, *Safeguarding of Controlled Unclassified Information*, requires contractors and subcontractors to provide adequate security to protect CUI from unauthorized access and disclosure. This includes

complying with DHS policies and procedures, accessible at *https://www.dhs.gov/dhs-security-and-training-requirements-contractors*, in effect when the contract is awarded.

As it relates to the information system security portion of the adequate security requirements, the process to obtain an ATO is clearly described in the text of clause 3052.204-7X, *Safeguarding of Controlled Unclassified Information.* The remaining adequate security requirements are documented in the policies and procedures on the publicly facing website. As such, no additional guidance on adequate security is required.

Comment: One respondent recommended that DHS establish mechanisms through which contractors can obtain sufficient clarity during the proposal stage both to determine whether CUI will be processed under the contract and, if yes, to assess whether they can comply with such safeguarding obligations.

Response: DHS shared this concern when developing the proposed rule and indicated as such in the preamble of the proposed rule by stating that feedback from industry consistently has indicated the need for transparency and clear and concise requirements as it relates to information security. This concern led DHS to establish in the proposed rule a process by which DHS contractors will be aware of the security requirements they must meet when responding to DHS solicitations that require a contractor to collect, process, store, or transmit CUI. Previously, information security requirements were either embedded in a requirements document (i.e., Statement of Work, Statement of Objectives, or Performance Work Statement) or identified through existing clause 3052.204-70, *Security Requirements for Unclassified Information Technology Requirements*. This approach: (1) created inconsistencies in the identification of information security requirements for applicable contracts; (2) required the identification and communication of security controls for which compliance was necessary after contract award had been made; and (3) resulted in delays in contract performance. Clause 3052.204-7X, *Safeguarding of Controlled Unclassified Information*, substantially

mitigates the concerns with DHS's previous approach. Through the government-provided Security Requirements Traceability Matrix (SRTM), contractors will know at the solicitation level the security requirements with which they must comply. The SRTM identifies the security controls that must be implemented on an information system that collects, processes, stores, or transmits CUI and that are necessary for the contractor to prepare its SA package. Clear identification of these requirements at the solicitation level affords contractors the ability to: (1) assess their qualifications and ability to fully meet the Government's requirements; (2) make informed business decisions when deciding to compete on the Government's requirements; and (3) engage subcontractors, if needed, early in the process to enable them to be fully responsive to the Government's requirements. The rule states that "[t]he SA package shall be developed using the government-provided Security Requirements Traceability Matrix and SA templates." Any concerns regarding the SRTM can be raised and resolved using traditional solicitation processes.

Comment: One respondent recommended that DHS consider implementing a review process for ensuring that contractors can propose alternative, but equally effective, controls, an approach used by DoD in its information safeguarding rulemaking. The respondent recommended that the process also include a procedure through which contractors can obtain confirmation that a particular control is unnecessary. The respondent also recommended that DHS clarify the process for making such determinations and that contractors be permitted to make such determinations on an individual basis.

Response: DHS declines these recommendations given that the ability for a contractor to engage on security measures included in the SRTM, which includes the applicability of the control and implementation method, is inherent in the Department's SA process. In addition, because the SRTM will be included in all applicable

solicitations, any concerns regarding the SRTM can be raised and resolved using traditional solicitation processes. As such, there is no need to add language to the clause to identify this capability.

Comment: One respondent stated that the government-supplied SRTM has the potential to be a useful tool to help ensure its members' ability to be responsive to the Government's security requirements. The respondent was unclear whether an SRTM will be provided with each solicitation or only in cases where a contractor will be operating an information technology (IT) system on behalf of the Government. The respondent requested that all DHS solicitations include: (1) a description of whether CUI Basic and/or CUI Specified information will be collected, processed, stored, or transmitted by the contractor on behalf of DHS during the course of the project; and (2) a list of applicable security requirements, including any requirements for CUI Specified information that must be protected on nonfederal information systems at higher than the CUI Basic "moderate" confidentiality level of the NIST SP 800–171 standards.

Response: The information system security requirements in this rule are focused on those applicable to Federal information systems, which include contractor information systems operated on behalf of the agency. As previously stated, the requirements applicable to nonfederal information systems will be addressed in the FAR CUI rule, and as such, they are not addressed in this rulemaking. For the purposes of the information systems subject to this rulemaking, an SRTM will be included in all applicable solicitations using the controls from NIST SP 800–53. The type(s) of CUI provided and/or developed under the contract also will be identified in the solicitation. Apart from using NIST SP 800–171 as a baseline for the security controls, DHS does not anticipate a change to the process of providing an SRTM and identifying the type(s) of CUI provided or developed under a contract where nonfederal information systems are used. However, this process cannot be fully defined until the FAR CUI rule is finalized.

Comment: One respondent raised concerns regarding the security review requirements of paragraph (c)(3) of clause 3052.204-7X, *Safeguarding of Controlled Unclassified Information*. The respondent stated that proper control of information is already outlined in the applicable law, regulation, and Governmentwide policy that applies to that information and that compliance with contract terms is already included in agreement terms. The commenter requested that DHS take an approach similar to DoD and either use existing FAR processes and procedures to facilitate these requirements or identify them at the contract level in lieu of specifying the requirements in the clause.

Response: The ability to perform periodic security reviews is an important mechanism for the Department to consistently ensure contractors are and remain compliant with the security requirements contained in their contracts. This is borne out by the prevalent and persistent nature of cyber-attacks against both public and private networks and information systems. Although the Department is reserving the right to perform random security reviews, the Department will be judicious in its use and will coordinate appropriately with contractors to ensure operations are not unduly impacted. It is also important to note that reciprocity among agency regulations is outside the scope of this rule.

5. CUI Registry

Comment: Several respondents raised concerns that the rule proposed included categories of CUI that are not included in the CUI Registry maintained by NARA. In support of these concerns, respondents cited various sections of 32 CFR part 2002, such as "[a]gencies may use only those categories or subcategories approved by the CUI EA [established by E.O. 13556 as NARA] and published in the CUI Registry to designate information as CUI." 32 CFR 2002.12(b).

Response: Based on the number of comments related to DHS's inclusion of new categories and subcategories of CUI in the proposed rule, it appears there is: (1) a

misperception among our industry partners that the CUI Registry cannot change; and (2) a misunderstanding of the process by which agencies can add new categories to the CUI Registry. The categories and subcategories of information in the CUI Registry are not static. E.O. 13556, *Controlled Unclassified Information*, establishes a process to add new categories and subcategories of CUI. DHS's addition of new CUI categories and subcategories is in line with the procedures established by E.O. that require that the category or subcategory of information be in a law, regulation, or Governmentwide policy. DHS proposed the new categories and subcategories of CUI through the regulatory process (i.e., its NPRM) and received provisional approval from NARA for the proposed categories. As a result of this approval, these categories now appear in the CUI registry.

Comment: One respondent advised that restating CUI categories increases administrative burdens. The same respondent also raised concerns that paragraph (b), *Handling of Controlled Unclassified Information*, of clause 3052.204-7X, *Safeguarding of Controlled Unclassified Information*, refers contractors back to DHS policies and procedures and advised that DHS should instead refer contractors to the CUI Registry and avoid duplicative descriptions of CUI. The respondent also stated that DHS defined Operations Security Information too broadly and that it could be interpreted to include almost any information. Multiple respondents raised the same concern about the Department's definition of Homeland Security Agreement Information. One respondent stated that the definition is vague and overly broad and does not comport with either the definition of CUI set forth in 32 CFR part 2002 or the categories or subcategories of CUI included in the CUI Registry, while other respondents stated that the definition allows DHS to determine what Homeland Security Agreement Information is on a case-by-case basis in individual contracts. Another stated that the parameters for Homeland Security

Agreement Information are very uncertain and seemingly could apply to any information included in such agreements.

Response: The CUI Registry does not describe safeguarding and dissemination requirements in sufficient detail to allow for general users to properly protect information without supplemental guidance. In most instances, it is only a citation of a law, regulation, or Governmentwide policy. With regard to Operations Security Information, the definition used in this regulation has been updated and is derived from the definition "Operations Security (OPSEC)" from National Security Presidential Memorandum 28, which was issued in January 2021. While agreeing that the category is broad, DHS also believes it necessary, much like other similarly broad categories, such as privacy and law enforcement information. DHS is unable to address it solely in specific contracts or project guidance as such a practice would by definition be an ad-hoc agency practice existing outside of a law, regulation, or Governmentwide policy and, thus, contrary to E.O. 13556. Instead, DHS opted to define this protection within the scope of this regulation.

With regard to Homeland Security Agreement Information, in furtherance of the Department's core missions of (1) preventing terrorism and enhancing security, (2) securing and managing the borders, (3) ~~Homeland Security Agreement Information~~ enforcing and administering immigration laws, (4) safeguarding and securing cyberspace, and (5) ensuring resilience to disasters, DHS enters into thousands of information sharing agreements with State, local, and private sector entities. The information being shared is often sensitive, thus requiring protections from public disclosure, but does not easily fall into one of the other CUI categories. DHS has historically protected this information as For Official Use Only, the DHS precursor to the CUI regime. While the definition of Homeland Security Agreement Information is admittedly broad, fulfilling core DHS missions while protecting sensitive information shared with DHS by our nonfederal

partners requires such flexibility. DHS finalizes the CUI categories as proposed and declines to make changes in response to public comments.

Comment: One respondent stated the rule does not discuss who has the responsibility to identify or designate DHS CUI; whether any safeguarding obligations also apply to other categories or subcategories of CUI as listed in the CUI Registry; what relationship must exist between the presence of information that could be CUI and a contractual obligation to DHS; or how the agency will respond, advise, or adjudicate any questions as to application, administration, implementation, or enforcement of the safeguarding obligation.

Response: The purpose of this rulemaking is to clearly identify contractor responsibilities with respect to safeguarding CUI and identify security requirements and processes applicable to Federal information systems, which include contractor information systems operated on behalf of the Government. Identification of individuals/organizations within the Department responsible for designating CUI and safeguards applicable to CUI does not achieve this end. Also, a specific process on how the agency will respond, advise, or adjudicate any questions as to application, administration, implementation, or enforcement of the safeguarding obligation is also unnecessary. Should an issue or concern arise, it can be handled through traditional contract administration practices.

6. DHS Internal Policies and Procedures

Comment: One respondent expressed concern that the "adequate security" requirements in paragraph (b), *Handling of Controlled Unclassified Information*, in clause 3052.204-7X, *Safeguarding of Controlled Unclassified Information*, refer to security standards in DHS-specific documents (as opposed to security standards designed for use across the executive branch) that are hosted on a DHS website. The respondent expressed concern that DHS may unilaterally change these security standards from time

to time, causing significant adverse effects to contractors without giving them a meaningful opportunity to comment on these changes. Based on this concern, the respondent proposed the following revision (revision in bold type):

> Adequate security includes compliance with DHS policies and procedures in effect at the time of contract award. These policies and procedures are accessible at *https://www.dhs.gov/dhs-security-and-training-requirements-contractors*. **Changes to policies and procedures will be identified by version controls and implementations of these new versions will only occur after the contractors affected by the change are allowed time to comment on changes that will affect a contract's cost and/or schedule.**

Response: DHS does not accept the recommendation to add language to clause 3052.204-7X, *Safeguarding of Controlled Unclassified Information*, documenting how and when updates to the Department's policies and procedures will be handled after a contract has been awarded. DHS employs version control on all internal policies and procedures. Contractors are not afforded the opportunity to comment on internal policies and procedures of Federal agencies when they are developed or when they are updated. Any impacts to DHS contractors as a result of updates to policies and procedures will be handled through the normal contract administration process, which already allows a contractor to assess the impact of the change and request consideration from the Government prior to implementation of the change. As such, there is no need to add specific language in the clause allowing a contractor to review and assess impacts to contract schedules and costs.

7. Definitions

Comment: Multiple respondents requested that DHS include the definition of "on behalf of an agency" consistent with 32 CFR part 2002. Another respondent stated that the rule does not clearly define the term "nonfederal information system" as storing or handling CUI only incidental to providing a service or product to the Government, nor does it apply "on behalf of an agency" in a manner consistent with 32 CFR part 2002.

Response: DHS intentionally excluded the "on behalf of an agency" definition provided in the NARA CUI rule from this rulemaking. The phrase "on behalf of an agency" is already rooted in statute and is used extensively in FISMA. FISMA designates the Director of the OMB as being responsible for "developing and overseeing the implementation of policies, principles, standards, and guidelines on information security . . . ." 44 U.S.C. 3553(a)(1). As such, any definition of the phrase "on behalf of an agency" must be provided in FISMA policy and guidance issued by OMB after going through the appropriate interagency coordination process to assess the wide-ranging implications of defining this term. In the case of the NARA CUI rule, that has not happened. In addition, the NARA CUI rule addresses a small subset of the issues covered by FISMA. For example, FISMA applies to all information, not just CUI. In addition, FISMA requires agencies to provide information security protections related to the integrity, confidentiality, and availability of all information (including CUI). The NARA CUI rule relates only to a subset of these concerns, specifically confidentiality of CUI.

The rule defines a Federal information system as "an information system used or operated by an agency or by a Contractor of an agency or by another organization on behalf of an agency." This definition was taken directly from OMB Circular A–130. Defining a Federal information system is sufficient for the purposes of this rulemaking as an information system, in the context of this rule, is either Federal or nonfederal. Including a definition of a nonfederal information system is not necessary as it logically follows that a nonfederal information system is the opposite of a Federal information system. Also, "nonfederal information system" is not defined in Governmentwide policy. Lastly, the information system security requirements of this rule are limited to Federal information systems.

8. Reciprocity in Interagency Regulations and Information Security Requirements

Comment: Multiple respondents raised concerns that the requirements of the rule are not the same as other rules related to CUI issued by other Departments and agencies, such as DoD, and requested that DHS revise this rule to be consistent with those rules. Respondents also stated that there is a lack of consistency between DHS and DoD incident reporting requirements on what constitutes timely reporting of breaches. Because companies often do work for multiple Federal agencies, the respondent stated that it is important to have a consistent approach Governmentwide so that companies can set up a single compliant system and process.

Response: Reciprocity in information security policies and regulations and incident reporting requirements among Departments and agencies is outside the scope of this regulation. The purpose of this rulemaking is to ensure that DHS contractors adequately protect CUI received under DHS contracts. As such, the focus of this rule is properly limited to the interests and mission needs of the Department. Additionally, this rule is fully consistent with all applicable statutes, regulations, and Governmentwide policies applicable to CUI and information systems. With regard to reciprocity in information security policies, DHS finalizes the rule as proposed and declines to make changes in response to public comments.

Comment: One respondent expressed concern that the rule fails to emphasize the need for reciprocity across Federal agencies and the requirement to rely upon provisional authorizations and ATOs already obtained through other Federal agencies.

Response: The focus of this rule is properly limited to the interests and requirements of DHS. As such, reciprocity across the Federal government and the requirement to rely upon provisional authorizations and ATOs obtained from other Departments and agencies is beyond the scope of this rule. However, nothing in the rule

prevents a contractor from submitting a SA package that was previously approved by another Department, agency, or DHS Component. DHS will consider existing SA packages and test results, as appropriate. It is quite possible that such a submission would expedite the approval process to obtain an ATO from DHS.

9. Incident Reporting and Response

Comment: Several respondents stated that the DHS requirement to report incidents involving PII or SPII within 1 hour of discovery, and all other incidents within 8 hours of discovery, is unreasonably short and inconsistent with other government requirements. One respondent stated that it is important to have a consistent approach Governmentwide so that companies can set up a single compliant system and process. One respondent recommended DHS extend the reporting timeframes to 8 hours for known incidents and 72 hours for suspected incidents involving contractors' internal information systems. One respondent suggested DHS extend the timeframe for reporting known or suspected incidents on contractor information systems not operated on behalf of the Department to 72 hours. Another respondent requested that DHS revise its incident reporting requirement to exclude reporting when the contractor information system is not operated on behalf of the Department.

Response: The requirement to report incidents impacting PII within 1 hour of discovery is documented in OMB memorandum M–18–02, *Fiscal Year 2017–2018 Guidance on Federal Information Security and Privacy Management Requirements*, and in United States Computer Emergency Readiness Team (US-CERT) Federal Incident Notification Guidelines. The 8-hour reporting timeline for incidents impacting all other categories of CUI came from the Department's review of its internal policies and procedures for other categories of CUI. Specifically, the Department reviewed its policies for chemical-terrorism vulnerability information (CVI), protected critical infrastructure information (PCII), and sensitive security information (SSI) (categories of information

for which the Department is statutorily responsible) and determined that the existing reporting timeline for incidents impacting these information categories is 8 hours. The Department considered creating a separate reporting timeline for PII, CVI, PCII, and SSI and establishing a different reporting timeline for the remaining categories of CUI and determined that having multiple reporting timelines would create confusion and could potentially result in incidents not being timely reported to the Department. It is also important to note that Departments and agencies must report information security incidents where the confidentiality, integrity, or availability of a Federal information system is potentially compromised to US-CERT within 1 hour of being identified by the agency's top-level Computer Security Incident Response Team, Security Operations Center (SOC), or IT department. As it relates to the incident reporting timelines required by DoD, reciprocity among agency regulations is outside the scope of this rule.

DHS does not accept the recommendation to extend the reporting requirement for known or suspected incidents on contractor information systems that are not operated on behalf of the Department (i.e., a nonfederal information system). The importance of CUI is not changed by being on a nonfederal information system. As such, DHS will not hold nonfederal information systems that contain the Department's CUI to a lower standard than Federal information systems that contain the same information.

DHS also does not accept the recommendation that incidents impacting CUI on a contractor's internal information systems should not be reported to the Department. A suspected or known incident impacting the Department's CUI should always be reported. To require anything less would be contrary to the public interest and the mission of the Department.

Comment: One respondent asked DHS to clarify that if a subcontractor experiences an incident, the subcontractor is required to submit the incident report to

DHS, but the subcontractor also must notify the prime contractor (or next higher tier contractor) that it submitted the report.

Response: DHS accepts this recommendation. DHS included paragraph (j), *Subcontracts*, in proposed clause 3052.204-7X, *Safeguarding of Controlled Unclassified Information*, to make clear that the requirements of the clause must be included in the terms and conditions of subcontract agreements, making subcontractors responsible for complying with the requirements of the clause. However, to make clear the Department's intent to require that subcontractors report incidents that occur in their facilities and information systems, DHS has revised proposed paragraph (d) (now paragraph (c)), *Incident Reporting Requirements*, to add subcontractor reporting responsibilities.

Comment: One respondent raised concerns that the incident response requirements in paragraphs (e)(3) and (5) of proposed clause 3052.204-7X, *Safeguarding of Controlled Unclassified Information*, state the following: "(3) Incident response activities determined to be required by the Government may include, but are not limited to, the following: (i) Inspections, (ii) Investigations . . ." and "(5) The Government, at its sole discretion, may obtain assistance from other Federal agencies and/or third-party firms to aid in incident response activities." The respondent recommended that the clause clarify how a contractor's confidential and privileged information will be protected in a case where the Government elects to conduct such inspections and investigations, particularly with the assistance of third-party firms.

Response: DHS does not accept the recommendation to identify in the text of the clause how a contractor's confidential and privileged information will be protected when third-party firms assist with the Department's incident response activities. However, DHS's current processes account for the protection of this information when third-party firms are used. DHS will continue to protect against the unauthorized use or disclosure of information received or obtained from contractors under clause 3052.204-7X,

Safeguarding of Controlled Unclassified Information. Contractors from third-party firms that assist in the Government's incident response activities are required to sign nondisclosure agreements. Additionally, both DHS and its contractors that report suspected or known incidents are required to complete a formal Rules of Engagement before incident response activities begin. The Rules of Engagement documents the security mechanisms that will be used to ensure the protection of information received during the Department's incident response activities.

Comment: One respondent stated that the incident reporting obligation does not limit the scope of reportable incidents to Federal information systems or even contractor information systems that contain Federal information. Because this distinction is not made, the respondent asserted that the rule could be read to require a contractor to report to DHS any incident impacting its own internal information systems, regardless of whether the incident has any likelihood of impacting the DHS CUI resident on that information system. The respondent recommended that DHS harmonize its reporting obligations with any reporting obligations currently under consideration by the FAR Councils in conjunction with its work on the FAR CUI rule.

Response: DHS disagrees that incidents should be reported to the Department only after the contractor determines it is likely the incident will impact/has impacted the DHS CUI resident on the information system. If DHS CUI is resident on an information system where a suspected or known incident occurs, contractors are required to report that incident to the Department. Additionally, it is clear from the title and substance of this rule that the focus is ensuring the adequate security of CUI, in general and when resident on an information system. To imply that this rule is requiring that suspected or known incidents must be reported on any and all information systems, including those that do not include the Department's CUI, is unreasonable and false. DHS is a participant

on the FAR team responsible for drafting the FAR CUI rule and has not identified any conflicts between this rule and the work taking place with the FAR team.

Comment: One respondent stated that the requirement to report all known and suspected incidents may result in a substantial number of false positives that would be unduly burdensome for both DHS and its contractors.

Response: The respondent is correct that the incident reporting requirements of the clause may result in a number of "false positives" being reported to the Department. DHS expects that this may be the case and is structured to receive and resolve the anticipated number of incidents to be reported under this clause. Given the persistent and prevalent nature of cyber-attacks against both public and private networks and information systems, it is increasingly imperative that the Department is timely notified of any suspected or known incidents impacting information systems where the Department's CUI resides.

Comment: One respondent stated that paragraphs (e), *Incident Response Requirements*, and (f), *PII and SPII Notification Requirements*, of proposed clause 3052.204-7X, *Safeguarding of Controlled Unclassified Information*, should be revised to be consistent with the current OMB directive. The *Discussion and Analysis* section of the proposed rule stated that "[t]he timing for reporting incidents involving PII or SPII is consistent with OMB Memorandum M–07–16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information." The respondent advised that the OMB memorandum cited was superseded on January 3, 2017, by OMB Memorandum M–17–12*, Preparing for and Responding to a Breach of Personally Identifiable Information*. The respondent recommended that DHS update the rule and proposed clause to reflect the current OMB memorandum.

Response: DHS accepts the recommendation and has updated the relevant portions of the rule to ensure consistency with OMB M–17–12, *Preparing for and Responding to a Breach of Personally Identifiable Information*.

10. Privacy Requirements

Comment: One respondent raised a concern regarding paragraph (b)(3) of proposed clause 3052.204-7X, *Safeguarding of Controlled Unclassified Information*, which prohibits a contractor from maintaining SPII in its invoicing, billing, and other recordkeeping systems. The respondent stated that some recordkeeping systems may have appropriate protections in place for safeguarding SPII while other systems may not. Because of this gap, the respondent recommended that contractors be required to protect SPII as required by law and be permitted to choose how best to meet that obligation given the nature of their information systems. The contractor also stated that the requirement would be prohibitive for an institution of higher education accepting a contract.

Response: DHS does not accept the respondent's recommendation. DHS has made a business decision based on previous incident response activities that DHS contractors are not authorized to maintain the Department's SPII in their invoicing, billing, and other recordkeeping systems.

Comment: One respondent raised concerns with paragraph (f)(1) of proposed clause 3052.204-7X, *Safeguarding of Controlled Unclassified Information*, which states that "[t]he Contractor shall not proceed with notification unless directed in writing by the Contracting Officer." The respondent expressed concern that the SPII or PII also might fall under the Health Insurance Portability and Accountability Act (HIPAA) or other Federal breach reporting requirements. If so, the respondent said, the language may present a conflict as to when and how to notify someone of the breach of their personal information. The respondent also stated that while it is unlikely that an institution would be notifying individuals of breaches within 5 days of the incident, an institution may

choose to notify another government official, such as the Secretary of Health and Human Services, if the incident also constitutes a breach under HIPAA. Because there is no other section of the clause clearly delineating the process to notify other governmental bodies, as may be required by State or Federal law, the respondent recommends revising the language as follows (revision in bold type):

> **The Contractor may notify other state or federal government agencies as required by law, but must copy the Contracting Officer on any reports made to other federal or state agencies**. The Contractor shall not proceed with notification **to individuals or entities outside of the government** unless directed in writing by the Contracting Officer.

Response: DHS partially accepts the recommendation. Proposed clause 3052.204-7X, *Safeguarding of Controlled Unclassified Information*, identifies requirements for reporting suspected or confirmed PII incidents as required by internal DHS policy and OMB memorandum M–17–12, *Preparing for and Responding to a Breach of Personally Identifiable Information*. Such requirements are identified in the DHS Incident Handling Guidance and are implemented in proposed clause 3052.204-7X, *Safeguarding of Controlled Unclassified Information*. Nonetheless, this clause was not intended to preempt contractors from reporting PII incidents under any applicable law. To ensure this point is clear, the statement was amended to add language allowing for compliance with applicable laws. Also, it is important to note the Department's timeline for notifying individuals pertains to when a contractor receives a notification request from the contracting officer; it is not related to the date the incident is reported.

Comment: One respondent recommended DHS consider extending the 5-day notification requirement to affected individuals to enable contractors to dedicate resources to remediation and investigation activities in the initial days after a breach. The respondent stated that the 5-day notification period is substantially shorter than most State reporting obligations (30–45 days in many States). The respondent asserted that many companies reflect these State time periods for providing notifications to affected

individuals and raised concerns that the notification timeline will detract from a contractor's ability to meaningfully respond to the incident.

Response: DHS does not accept the recommendation. The Department is requiring that contractors **notify the individual** whose PII and/or SPII was under the control of the contractor or resided in its systems at the time of the incident **not later than 5 business days after being directed to notify individuals, unless otherwise approved by the Contracting Officer** (emphasis added). The 5-business day notification period is only to address the time period in which the contractor must prepare and mail the notification to the individual, after being directed to do so by the Contracting Officer. It is completely unrelated to the timing of incident notification.

Comment: One respondent raised concerns with paragraph (g), *Credit Monitoring Requirements*, of proposed clause 3052.204-7X, *Safeguarding of Controlled Unclassified Information*. The section requires the contractor to provide credit monitoring services, including call center services, if directed by the Contracting Officer, to any individual whose PII or SPII was under the control of the contractor, or resided in the information system, at the time of the incident for a period beginning the date of the incident and extending not less than 18 months from the date the individual is notified. The respondent recommends that contractor's internal information systems be excepted from this requirement.

Response: DHS does not accept the recommendation to exclude contractor information systems from the credit monitoring requirements in clause 3052.204-7X, *Safeguarding of Controlled Unclassified Information*. The respondent is attempting to draw a distinction where there is none. Unauthorized access to or disclosure of the Department's PII on a contractor's internal information system has the same level of importance and potential impact as it would on a Federal information system. To the extent a contractor's internal information system contains PII provided by the

Government or generates PII on behalf of the Government and is subject to a known or suspected incident that impacts the PII, the contractor is responsible for providing notification and credit monitoring if the Government determines it is appropriate to do so. Any stance to the contrary is inconsistent with the public interest and the mission of the Department.

Comment: One respondent stated that the HSAR should include a requirement that the DHS procuring activity and the contractor explicitly agree on whether and to what extent the contractor has credit monitoring and call center obligations as part of a specific contract. The respondent stated that the agreement should specifically clarify whether these obligations extend to the contractor in relation to GFE that the contractor operates in its own internal contractor environment.

Response: Paragraphs (f), *PII and SPII Notification Requirements*, and (g), *Credit Monitoring Requirements*, of proposed clause 3052.204-7X, *Safeguarding of Controlled Unclassified Information*, state that those requirements are only applicable when an incident involves PII or SPII. To ensure that contractors understand when these requirements are applicable, DHS is making these requirements a separate clause at 3052.204-7Y titled *Notification and Credit Monitoring Requirements for Personally Identifiable Information Incidents*. The applicability of new clause 3052.204-7Y, *Notification and Credit Monitoring Requirements for Personally Identifiable Information Incidents*, is limited to solicitations and contracts where a contractor will have access to PII. This change ensures DHS contractors understand credit monitoring and notification requirements are only applicable when the solicitation and contract require contractor access to PII.

The decision to provide notification and credit monitoring services is specific to each incident. As such, a blanket determination cannot be made that these services will be required each time a known or suspected incident is reported that impacts PII. The intent

of the clause is to ensure that the Government can timely notify individuals impacted by an incident and provide them with credit monitoring services if and when the Government determines it is appropriate to do so. Paragraph (b)(2) of clause 3052.204-7Y, *Notification and Credit Monitoring Requirements for Personally Identifiable Information Incidents*, states that "[a]ll determinations by the Department related to notifications to affected individuals and/or Federal agencies and related services (e.g., credit monitoring) will be made in writing by the Contracting Officer." Therefore, the Contracting Officer will advise contractors of their requirements depending on the incident on a case-by-case basis. Depending on the severity of the incident, credit monitoring may not be necessary in one instance, but may be in another.

11. Sanitization of Government and Government-Activity-Related Files and Information

Comment: One respondent questioned the implementation of paragraph (h), *Certificate of Sanitization of Government and Government-Activity-Related Files and Information*, of proposed clause 3052.204-7X, *Safeguarding of Controlled Unclassified Information*. The clause states "the Contractor shall return all CUI to DHS and/or destroy it physically and/or logically as identified in the contract." The respondent asked where such information would be identified in the contract, specifically whether the information would be identified in the clause, the Statement of Work, or some other attachment. The respondent also stated that it would be helpful to see the DHS language that identifies how a contractor is to destroy CUI physically and/or logically.

Response: DHS will identify in the Statement of Work, Statement of Objectives, Performance Work Statement, or specification if and when CUI is required to be returned, physically and/or logically destroyed, or both. Clause 3052.204-7X, *Safeguarding of Controlled Unclassified Information*, states that destruction of the CUI "shall conform to the guidelines for media sanitization contained in NIST SP 800–88,

Guidelines for Media Sanitization." As such, no additional instruction on how to physically or logically destroy CUI is necessary.

Comment: One respondent noted that the sanitization requirement is contrary to data use rights typical for an institution of higher education environment. The respondent stated that it is very common for higher education institutions to maintain files and data associated with research under U.S. Government contracts and grants that will be used for follow-on research and that CUI may be resident on contractor information systems. The respondent recommended that the language be revised to indicate that the contractor must return or destroy the CUI when it is specified by the individual contract. The respondent also recommended DHS use the requirements under NIST SP 800–171, which includes a media sanitization protocol.

Response: Proposed paragraph (h), *Certificate of Sanitization of Government and Government-Activity-Related Files and Information*, requires contractors to return all CUI to DHS and/or destroy it physically and/or logically using the guidelines in NIST SP 800-88, Guidelines for Media Sanitization. Contractors must also certify and confirm sanitization and submit the certification to the COR and contracting officer.

However, to ensure that media is returned and destroyed only when the Government has determined it to be appropriate to do so, the language is revised to state that CUI must be returned and/or destroyed **unless** the contract states that return or destruction of CUI is not required. Also, the media sanitization requirements in the clause do not conflict with the media sanitization protocols in NIST SP 800–171 as the sanitization requirements in this publication are taken from NIST SP 800–88.

12. Subcontractor Flow-down Requirements

Comment: Multiple respondents expressed concern that paragraph (j), *Subcontracts*, of proposed clause 3052.204-7X, *Safeguarding of Controlled Unclassified Information*, requires contractors to "insert this clause in all subcontracts and require

subcontractors to include this clause in all lower-tier subcontracts." The respondent stated that this language appears to require contractors to flow down the clause to subcontractors that have no role in receiving or creating CUI in performance of the contract. The respondent stated that this is inconsistent with the applicability described in the preamble to the proposed rule and recommended that the language be updated accordingly.

Response: DHS agrees with the recommendation. Proposed paragraph (j) (now paragraph (g)), *Subcontracts*, has been revised to require contractors flow down the clause only to subcontracts involving CUI.

13. Requirements Applicable to Educational Institutions

Comment: One respondent noted that paragraph (a) of proposed clause 3004.470-4 states that "[n]either the basic clause nor its alternates should ordinarily be used in contracts with educational institutions." The respondent stated that it would be helpful for DHS to indicate what specific contract clauses they expect to use with educational institutions, and what controls (such as, for example, those described in NIST SP 800–171) would be required to be in place to protect CUI information received pursuant to those clauses. The respondent recommended that, in the case of contracts requiring an institution of higher education to have access to CUI, or to collect or maintain CUI on behalf of the agency, DHS use the baseline requirement of "moderate" security controls for CUI Basic information, as described in NIST SP 800–171. The respondent stated that protections required in addition to those present under CUI Basic should be implemented through the CUI Registry's CUI Specified mechanisms to reflect the requirements of applicable law, regulations, or Governmentwide policy requiring supplemental controls, and should be specifically identified in the governing contract. The respondent also requested that information that does not meet the definition of CUI, such as vendor proprietary information, be specifically identified in the contract, along with the level of

protection that must be afforded to such information. The respondent stated that this approach would reduce the substantial administrative and financial burdens to the institutions, funding agencies, and their external partners and will allow institutions of higher education to adopt the compliance solutions that work best with their existing information systems and practices.

Response: The statement that "[n]either the basic clause nor its alternates should ordinarily be used in contracts with educational institutions" is only applicable to clause 3052.204-71, *Contractor Employee Access*. It is also important to note that this statement does not prohibit the Department from including the clause or its alternates in contracts with educational institutions when it is determined to be necessary. The recommendation that DHS should indicate what specific contract clauses it expects to use and security controls required to be in place to protect CUI when contracting with educational institutions implies the Department should use a lesser information security standard when contracting with these organizations. This is not the case. The security requirements required are those discussed in this rule. Additionally, information that is neither CUI nor classified is not required to be protected.

As previously stated, Federal information systems, which include contractor information systems operated on behalf of the agency, are subject to the requirements of NIST SP 800–53. Generally speaking, should the Government determine that a contractor information system is not operated on its behalf, NIST SP 800–171 is applicable instead of NIST SP 800–53. However, consistent with 32 CFR 2002.14(a)(3) and (g), "[a]gencies may increase CUI Basic's confidentiality impact level above moderate only internally, or by means of agreements with agencies or non-executive branch entities (including agreements for the operation of an information system on behalf of the agencies)." Relatedly, 32 CFR 2002.4(c) states that agreements "include, but are not limited to, contracts, grants, licenses, certificates, memoranda of agreement/arrangement or

understanding, and information-sharing agreements or arrangements." Therefore, DHS can require a confidentiality impact level above moderate through agreements with non-executive branch entities and does not need an update to the CUI Registry to do so. DHS will determine if an information system is Federal or nonfederal, perform the necessary risk assessment consistent with Departmental policy, and identify the security controls contractors must meet through an SRTM. The SRTM will be included in the solicitation to ensure contractors clearly understand the security requirements they must meet before responding to the solicitation. Apart from using NIST SP 800–171 as a baseline for the security controls, DHS does not anticipate a change to the process of providing an SRTM and identifying the type(s) of CUI provided or developed under a contract where nonfederal information systems are used. However, this process cannot be fully defined until the FAR CUI rule is finalized.

14. Self-deleting Requirements

Comment: DHS invited comments on the self-deleting requirements in proposed clause 3052.204-7X, *Safeguarding of Controlled Unclassified Information*. One respondent raised concerns with the use of self-deleting requirements and requested that DHS consider the use of alternates to help parties achieve certainty about their responsibilities to implement the requirements of the clause.

Response: DHS agrees with the commenter that the use of alternates will increase certainty among DHS contractors on their responsibilities to comply with the requirements of clause 3052.204-7X, *Safeguarding of Controlled Unclassified Information*. As such, DHS has: (1) made the requirements of paragraph (c), *Authority to Operate*, Alternate I to the basic clause 3052.204-7X, *Safeguarding of Controlled Unclassified Information*; and (2) made the requirements of paragraphs (f), *PII and SPII Notification Requirements*, and (g), *Credit Monitoring Requirements*, a separate clause at

3052.204-7Y titled *Notification and Credit Monitoring Requirements for Personally Identifiable Information Incidents*.

As a result of these changes, basic clause 3052.204-7X, *Safeguarding of Controlled Unclassified Information*, is limited to the following provisions: paragraphs (a), *Definitions*; (b), *Handling of Controlled Unclassified Information*; (c), *Incident Reporting Requirements*; (d), *Incident Response Requirements*; (e), *Certification of Sanitization of Government and Government-Activity-Related Files and Information*; (f), *Other Reporting Requirements*; and (g), *Subcontracts*. Compliance with these requirements is mandatory regardless of the information system type (i.e., Federal information system or nonfederal information system). Alternate I to the basic clause is applicable when Federal information systems, which include contractor information systems operated on behalf of the agency, are used to collect, process, store, or transmit CUI. New clause 3052.204-7Y, *Notification and Credit Monitoring Requirements for Personally Identifiable Information Incidents*, is applicable to solicitations and contracts where a contractor will have access to PII. These changes were made to: (1) ensure DHS contractors clearly understand the scope and applicability of the various requirements contained in clause 3052.204-7X, *Safeguarding of Controlled Unclassified Information*; (2) make clear that the ATO requirements of the clause are only applicable to Federal information systems, which include contractor information systems operated on behalf of the agency; and (3) ensure DHS contractors understand credit monitoring and notification requirements are only applicable when the solicitation and contract require contractor access to PII.

15. Applicability to Service Contracts

Comment: The proposed rule requested comments on making proposed clause 3052.204-7X, *Safeguarding of Controlled Unclassified Information*, applicable to all service contracts with the understanding that the clause would be self-deleting if it does

not apply. One respondent stated that it would be preferable for DHS to include the clause only in those contracts where the clause is required, saying there is no realistic self-deleting function.

Response: DHS agrees with the commenter and will not make the requirements of the proposed rule applicable to all service contracts. Clause 3052.204-7X, *Safeguarding of Controlled Unclassified Information*, will be included only in contracts where its requirements are applicable.

16. Costs

Comment: One respondent noted that the cost data provided in the proposed rule are based on the assumption of a contractor having a centralized system base (for example, one information system, one accounting system, a limited number of individuals with access, a controlled physical environment). The respondent stated that institutions of higher education are highly decentralized entities and that costs increase significantly when implementing these requirements over multiple systems, on a case-by-case basis, as would generally be required in the decentralized higher education environment. The respondent said the problem only is magnified when each agency adopts separate and distinct requirements for the safeguarding of CUI, making it imperative to have one standard to operate by, such as that proposed under the NARA CUI rule.

Response: The information system security requirements of this rule are focused on the requirements applicable to Federal information systems. Requirements for Federal information systems are governed by Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*; FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*; and NIST SP 800–53, *Security and Privacy Controls for Information Systems and Organizations*. These publications define the

process by which the Government categorizes a Federal information system as requiring low, moderate, or high security controls to protect the confidentiality, integrity, and availability of information that is processed, stored, and transmitted by those systems/organizations and to satisfy a set of defined security requirements. The commenter's approach displaces compliance with these publications and requests that the Government identify a single security standard for Federal information systems without the benefit of the methodical and deliberate processes required by each of these publications. This approach is unacceptable because it is inconsistent with FISMA and NIST policy for Federal information systems. Alternatively, the NARA CUI rule establishes baseline information security requirements necessary to protect CUI Basic on nonfederal information systems by mandating the use of NIST SP 800–171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*, when establishing security requirements to protect CUI's confidentiality on nonfederal information systems. However, consistent with 32 CFR 2002.14(a)(3) and (g), "[a]gencies may increase CUI Basic's confidentiality impact level above moderate only internally, or by means of agreements with agencies or non-executive branch entities (including agreements for the operation of an information system on behalf of the agencies)."

The Department has not updated cost estimates to account for institutions with multiple systems because, based on Federal Procurement Data System (FPDS) data on unique vendors awarded contracts under the most likely applicable Product and Service Codes (PSCs) in Fiscal Year (FY) 2019 and FY 2020, fewer than 1 percent of affected entities are educational institutions that could have multiple systems. Based on the estimated population of affected entities (171), only one entity would be an educational

institution that might have multiple systems on average.[4] In addition, DHS has no data on how many systems these entities use. Other types of entities could have multiple systems. However, multiple variables dictate the cost of an independent assessment (e.g., governance, decentralization of information systems, number of information systems (i.e., size), complexity, categorization, and documentation). As such, the number of information systems impacted by the ATO is not the sole factor to consider when determining if there will be increases to the cost of an independent assessment. While there may be increases to the cost of an independent assessment when multiple information systems are involved, such increases are largely dependent upon the level of decentralization of the systems and variances in the governance structure of each system. If the information systems have the same or similar governance structures, the cost of the independent assessment may not see significant cost impacts. Conversely, if there is significant decentralization and variances in governance structures, the cost of an independent assessment could increase. Such determinations must be made on a case-by-case basis and take into consideration all relevant factors that dictate the cost of an independent assessment.

Therefore, DHS maintains the cost estimates from the proposed rule but recognizes that these costs may be underestimates because FPDS data do not indicate subcontractors that may have multiple systems, and there is uncertainty on the prevalence of multiple systems for affected entities beyond educational institutions and uncertainty related to the cost implications to independent assessment of multiple systems.

IV. Statutory and Regulatory Requirements

[4] Calculation: 171 ATO vendors * 0.72 percent of educational institutions in the population = 1.2 ATO vendors with multiple systems.

A. Executive Orders 12866 and 13563

E.O. 12866 (Regulatory Planning and Review) and E.O. 13563 (Improving Regulation and Regulatory Review) direct agencies to assess the 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 has been designated a "significant regulatory action," although not economically significant, under section 3(f) of E.O. 12866. Accordingly, the rule has been reviewed by OMB.

1. Outline of the Analysis

Section IV.A.2.a describes the need for the final rule, and section IV.A.2.b describes the process used to estimate the costs of the rule and the general inputs used, such as the number of affected entities. Section IV.A.3 explains how the provisions of the final rule will result in quantifiable costs and presents the calculations DHS used to estimate them. In addition, section IV.A.3 describes the qualitative costs, cost savings, and benefits of the final rule. Section IV.A.4 summarizes the estimated first year and 10-year total and annualized costs of the final rule. Finally, section IV.A.5 presents the regulatory alternatives considered.

2. Summary of the Analysis

DHS expects that the final rule will result in costs, cost savings, and benefits. As shown in Exhibit 1, DHS estimates a range of costs to capture uncertainty in cost data and, therefore, presents the estimated impacts using a lower bound, upper bound, and primary estimate. The primary estimate is calculated by taking the average of the upper bound and lower bound estimates. DHS estimates the final rule will have an annualized cost ranging from $15.32 million to $17.28 million at a discount rate of 7 percent and a

total 10-year cost that ranges from $107.62 million to $121.37 million at a discount rate of 7 percent. DHS was unable to quantify the cost savings or benefits associated with the rule. However, the final rule is expected to produce cost savings by reducing the time required to grant an ATO, reducing DHS time reviewing and reissuing proposals because contractors are better qualified, and reducing the time to identify a data breach. The final rule also produces benefits by better notifying the public when their data are compromised, requiring the provision of credit monitoring services so that the public can better monitor and avoid costly consequences of data breaches, and reducing the severity of incidents through timely incident reporting.

Exhibit 1: Estimated Monetized Costs of the Final Rule ($2020 millions)

	Costs		
	Low	**Primary**	**High**
Undiscounted 10-Year Total	$152.60	$162.32	$172.04
10-Year Total with Discount Rate of 3%	$130.28	$138.58	$146.889
10-Year Total with Discount Rate of 7%	$107.62	$114.49	$121.37
Annualized with Discount Rate of 3%	$15.27	$16.25	$17.22
Annualized with Discount Rate of 7%	$15.32	$16.30	$17.28

Exhibit 2 below provides a detailed summary of the final rule provisions and their impacts. *See* the costs and cost savings subsections of section IV.A.3 (Subject-by-Subject Analysis) below for more detailed explanations.

Exhibit 2: Summary of Provisions and Economic Impacts of the Final Rule					
3052.204-7X, *Safeguarding of Controlled Unclassified Information*	**Requirement(s)**	**Expressly Required by Statute, Regulation, or Governmentwide Policy?**	**Statute, Regulation, or Governmentwide Policy**	**Costs**	**Benefits**
(a) Definitions	Defines terms applicable to the clause	N/A	Definitions for adequate security, Homeland Security Agreement Information, Homeland Security Enforcement Information, Operations Security Information, Personnel Security Information, and Sensitive Personally Identifiable Information are the only terms that are not defined in a statute, regulation, or Governmentwide policy	No costs associated with definitions	
(b) Handling of Controlled Unclassified Information	a) Requires contractors to comply with DHS policies and procedures for the handling of CUI	a) Yes	a) 32 CFR part 2002, *Controlled Unclassified Information (CUI)*	a) No new costs, is currently a regulatory requirement	Unquantified cost savings to DHS from clarified system requirements, which reduce time to grant ATOs, identify better qualified bidders for DHS contracts, and prevent DHS from putting contracts on hold to reissue requests for proposals and alternate contractors
	b) Limits contractors' use or redistribution of CUI to only those activities specified in the contract	b) No	b) N/A – Internal DHS requirement	b) Imposes no new cost	
	c) Ensures CUI transmitted via email is protected by encryption or transmitted within secure communications systems	c) No	c) N/A – Internal DHS requirement	c) Imposes no new cost	
(c) Incident Reporting Requirements	Contractors and subcontractors must: (a) Report all known or suspected incidents involving PII or SPII within 1 hour of discovery	a) Yes	a) OMB Memorandum M–17–12 PRIV, *Preparing for and Responding to a Breach of Personally Identifiable Information*, requires each agency to have a breach response plan that includes timely reporting. The DHS Senior Agency Official for Privacy	a, b) The primary estimate of reporting an incident to DHS is $1,075 per incident. DHS cannot quantify the aggregate total of these costs because DHS does not track the origin of security event notices and is therefore unable to determine how many	a, b, c) Timely reporting of incidents is critical to prevent the impact of an incident from expanding, ensure incident response and mitigation activities are undertaken quickly, and ensure individuals are timely notified of the possible or actual compromise of their PII.

			determined that to meet the timeliness requirements of M–17–12, the initial report must occur within 1 hour of discovery.	security event notices external contractors reported to their respective Component SOC or the DHS Network Operations Security Center.	Reducing the time to identify a breach improves the effectiveness of incident management, reduces false positives, improves triage by lowering the cost of trivial true positives, minimizes mission disruption and the resulting impact on revenue and performance, and reduces the cost of investigation.
	(b) Report all other incidents within 8 hours of discovery	b) No, internal policy requirement	b) N/A		
	(c) Ensure CUI transmitted via email is protected by encryption or transmitted within secure communications systems	c) No	c) 32 CFR 2002.14, *Safeguarding*, paragraphs (c), *Protecting CUI under the control of an authorized holder*, and (g), *Information systems that process, store, or transmit CUI*	c) No new costs, is currently a regulatory requirement	
(d) Incident Response Requirements	a) Requires contractors and subcontractors to provide full access and cooperation for all activities determined by the Government to be required to ensure an effective incident response	a) Yes	a) Federal Information Security Modernization Act of 2014 (44 U.S.C. 3551), OMB A–130, *Managing Information as a Strategic Resource*	a) DHS components have included differing language in contracts for incident response, while this provision creates consistency across DHS components in language without change to requirements. Since DHS already conducts this practice, these costs are part of the existing baseline costs of business.	Standardizing incident reporting leads to more proactive incident response, potentially faster incident resolution, and potential reduction in the scope and impact of the incident depending on the nature of the attack (i.e., fewer records breached)
	b) Allows the Government to obtain outside assistance to assist in incident response activities	b) No	b) N/A – Internal DHS requirement	b) N/A – The Government bears the costs related to obtaining assistance from external parties for incident response activities (e.g., existing DHS contracts, interagency agreements). This cost is not new because incident response is a longstanding practice and DHS has existing pre-position contracts that allow it to tap services for incident response.	

(e) Certificate of Sanitization of Government and Government-Activity-Related Files and Information	Requires the contractor to return all CUI to DHS and/or destroy it physically and/or logically. Destruction must conform to the guidelines for media sanitization contained in NIST SP 800–88, *Guidelines for Media Sanitization*.	Yes	Paragraph (d) of HSAR 3052.204-70, *Security Requirements for Unclassified Information Technology Resources*	No new costs are anticipated as this requirement simply replaces the pre-existing requirement in paragraph (d) of HSAR 3052.204-70, *Security Requirements for Unclassified Information Technology Resources*. Additionally, any costs associated with this requirement are covered under the initial regulation for HSAR 3052.204-70, *Security Requirements for Unclassified Information Technology Resources*.	
(f) Other Reporting Requirements	Informs contractors that the incident reporting required by this clause does not rescind the contractor's responsibility for other incident reporting pertaining to its unclassified information systems under other clauses that may apply to its contract(s), or as a result of other applicable statutory or regulatory requirements, or other U.S. Government requirements	No	N/A	No costs related to DHS are anticipated with this requirement as those costs would be covered under the "other applicable statutory or regulatory requirements, or other U.S. Government requirements"	
(g) Subcontracts	Requires the contractor to insert this clause in all subcontracts and require subcontractors to include this clause in all lower tier subcontracts when subcontractor employees will have access to CUI; CUI will be collected or maintained on behalf of the agency by a subcontractor; or a	In part. Prime contractors are required to flow down the text of this clause to applicable subcontracts. Many of the clause requirements stem from a statute, regulation, or Governmentwide	See above and below		

	subcontractor information system(s) will be used to process, store, or transmit CUI	policy as indicated above and below.			
(h) Authority to Operate	a) Security Authorization	a) Yes	a) Federal Information Security Modernization Act of 2014 (44 U.S.C. 3551), OMB A–130, *Managing Information as a Strategic Resource*, OMB Memorandum M–22–01, *Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response*, NIST SP 800–53, Revisions 4 and 5, *Security and Privacy Controls for Information Systems and Organizations*, and paragraphs (a) and (e) of HSAR 3052.204-70, *Security Requirements for Unclassified Information Technology Resources*	a) No new costs are anticipated as this requirement simply replaces the pre-existing requirement in paragraphs (a), (b), and (e) of HSAR 3052.204-70, *Security Requirements for Unclassified Information Technology Resources*. As part of the existing paragraphs (a) and (e) of HSAR 3052.204-70, *Security Requirements for Unclassified Information Technology Resources*, vendors are required to maintain full-time equivalent (FTE) oversight that is estimated to cost $209,008 per vendor.	
	b) Independent Assessment	b) No	b) N/A	b) $71.28 million at a 7% discount rate associated with the cost of an independent third party validating the security and privacy controls in place for the information system(s); reviewing and analyzing the SA package; and reporting on technical, operational, and management level deficiencies	Independent assessment provides an objective measure of compliance with security and privacy controls. Benefits of using a third party to perform an independent assessment extend to contractor because they can use results to demonstrate cybersecurity excellence for customers.
	c) ATO Renewal	c) Yes	c) See response at paragraph a)	c) No new costs are anticipated as this	

				requirement simply replaces the pre-existing requirement in paragraphs (a), (b), and (e) of HSAR 3052.204-70, *Security Requirements for Unclassified Information Technology Resources*. Additionally, any costs associated with this requirement are covered under the initial regulation for HSAR 3052.204-70, *Security Requirements for Unclassified Information Technology Resources*.	
	d) Security Review	d) No	d) N/A	d) $159,924 at a 7% discount rate from a new cost to the government to conduct the security reviews and to the contractor for any interruptions to normal operations caused by the security review	d) Security review is an important mechanism for the Department to consistently ensure contractors are and remain compliant with the security requirements contained in their contracts
	e) Federal Reporting and Continuous Monitoring Requirements	e) Yes	e) Federal Information Security Modernization Act of 2014 (44 U.S.C. 3551), OMB A–130, *Managing Information as a Strategic Resource*, OMB Memorandum M–14–03, *Enhancing the Security of Federal Information and Information Systems*, and NIST SP 800–53, Revisions 4 and 5, *Security and Privacy Controls for Information Systems and Organizations*	e) No new costs are anticipated as this requirement simply replaces the pre-existing requirement in paragraphs (a) and (e) of HSAR 3052.204-70, *Security Requirements for Unclassified Information Technology Resources*. Additionally, any costs associated with this requirement are covered under the initial regulation for HSAR 3052.204-70, *Security Requirements for Unclassified Information Technology Resources*.	
3052.204-7Y, *Safeguarding of Controlled*	**Requirement(s)**	**Expressly Required by Statute,**	**Statute, Regulation, or Governmentwide Policy**	**Costs**	**Benefits**

Unclassified Information		**Regulation, or Governmentwide Policy?**			
(a) Definitions	Defines terms applicable to the clause	No	Definition for Sensitive Personally Identifiable Information is not defined in a statute, regulation, or Governmentwide policy	No costs associated with definition	
(b) PII and SPII Notification Requirements	Requires the contractor, when directed, to notify any individual whose PII or SPII was either under the control of the contractor or resided in an information system under control of the contractor at the time the incident occurred	Yes	OMB Memorandum M–17–12, *Preparing for and Responding to a Breach of Personally Identifiable Information*	Estimated costs of notification are $2.72 per year per individual. DHS cannot quantify an aggregate total of this cost due to the rule because DHS does not track at the Department level the number of notifications required on either an annual or per-incident basis. **Note:** These costs are discretionary as the Government may or may not choose to have the contractor perform these services.	Benefit of improved notification to the public regarding breaches of their data, allowing better self-monitoring for identity theft. Such notification affords individuals the opportunity to take steps to minimize any harm associated with unauthorized or fraudulent activity.
(c) Credit Monitoring Requirements	Requires the contractor, when directed, to provide credit monitoring services to individuals whose PII or SPII was under the control of the contractor, or resided in the information system at the time of the incident, for a period beginning the date of the incident and extending not less than 18 months from the date the individual is notified.	Yes	OMB Memorandum M–17–12, *Preparing for and Responding to a Breach of Personally Identifiable Information*	Credit monitoring is estimated to cost $6.53 per year per individual. DHS cannot quantify these costs because it does not have estimates for the population of individuals affected. **Note:** These costs are discretionary as the Government may or may not choose to have the contractor perform these services.	Credit monitoring services can be particularly beneficial to the affected public as they can assist individuals in the early detection of identity theft as well as notify individuals of changes that appear in their credit report, such as creation of new accounts, changes to their existing accounts or personal information, or new inquiries for credit. Such notification affords individuals the opportunity to take steps to minimize any harm associated with unauthorized or fraudulent activity.

3052.204-71, *Contractor Employee Access*	**Requirement(s)**	**Expressly Required by Statute, Regulation, or Governmentwide Policy?**	**Statute, Regulation, or Governmentwide Policy**	**Costs**	**Benefits**
(a) Controlled Unclassified Information	Provides definition of CUI	N/A	Definitions for Homeland Security Agreement Information, Homeland Security Enforcement Information, Operations Security Information, Personnel Security Information, and Sensitive Personally Identifiable Information are the only terms that are not defined in a statute, regulation, or Governmentwide policy	N/A – No new costs are anticipated with the changes to this clause as the changes are merely updates to terminology and clarifying edits to ensure complete understanding of pre-existing requirements. Additionally, the costs associated with this clause are covered under the initial regulation for HSAR 3052.204-71, *Contractor Employee Access*.	
(b) Information Resources	Provides definition of information resources	N/A	Definition is taken from statute	No costs associated with definitions	
(c) Background Investigation Requirements	Identifies background investigation requirements	Yes	Paragraph (c) of HSAR 3052.204-71, *Contractor Employee Access*. **Note:** Paragraph was updated in final rule to replace the term "IT resources" with "information resources."	No new costs, is currently a regulatory requirement	
(d) Prohibition	Identifies circumstances where the contracting officer can prohibit individuals from working under a contract	Yes	Paragraph (d) of HSAR 3052.204-71, *Contractor Employee Access*. **Note:** No change from original text.	No new costs, is currently a regulatory requirement	
(e) CUI Disclosure and Training Requirements	Identifies limitation on disclosure of CUI and training requirements	Yes	Paragraph (e) of HSAR 3052.204-71, *Contractor Employee Access*. **Note:** Replaced references to "sensitive information" with "CUI" and clarified the timing for completion of training discussed in the original clause.	No new costs, is currently a regulatory requirement	

(f) Subcontract Requirements	Identifies when clause must be included in subcontracts	Yes	Paragraph (f) of HSAR 3052.204-71, *Contractor Employee Access*. **Note:** Replaced reference to "sensitive information" with "CUI" and "resources" with "information resources."	No new costs, is currently a regulatory requirement. **Note:** The change in terminology from "sensitive information" to "CUI" does not change the requirement for safeguarding. This change was made solely to comply with E.O. 13556, *Controlled Unclassified Information*, and its implementing regulation at 32 CFR part 2002. The type(s) of information DHS protected under "sensitive information" and now under "CUI" is not changed. Additionally, cost impacts associated with Governmentwide implementation of the CUI Program will be captured under the Federal Acquisition Regulation rulemaking that is currently in progress.	
(g) Training and Non-Disclosure Agreement Requirements	Identifies that contractors must complete a security briefing, additional training for specific categories of CUI (if identified in the contract), and sign a nondisclosure agreement before receiving access to information resources under the contract	Yes	Paragraph (g) of HSAR 3052.204-71, *Contractor Employee Access*. **Note:** Added language to clarify that additional training for specific categories of CUI from paragraph (e) will be identified in the contract.	No new costs, is currently a regulatory requirement	
(h) Contractor Access to Information Resources	Identifies restrictions on access to DHS information resources and consequences for attempting to access information resources that are not authorized under the contract	Yes	Paragraph (h) of HSAR 3052.204-71, *Contractor Employee Access*. **Note:** Replaced reference to "information technology resources" with "information resources."	No new costs, already a regulatory requirement	

(i), (j), (k), and (l)	No change from original clause text	Yes	Paragraphs (i), (j), (k), and (l) of HSAR 3052.204-71, *Contractor Employee Access*. **Note:** No change from original clause text.	No new costs, is currently a regulatory requirement	

a. Need for Regulation

DHS has determined that rulemaking is needed to implement security and privacy measures to safeguard CUI and facilitate improved incident reporting to DHS. The final rule enables DHS to identify, remediate, mitigate, and resolve incidents when they occur, not necessarily completely prevent them. DHS understands that there is no "true" way to completely prevent an incident from occurring. However, these measures are intended to decrease the likelihood of occurrence with full knowledge that there is no such thing as an "unhackable" system.

The final rule adds a new clause at 3052.204-7X, *Safeguarding of Controlled Unclassified Information*, that ensures adequate protection of CUI. That new clause (1) identifies CUI handling requirements and security processes and procedures applicable to Federal information systems, which include contractor information systems operated on behalf of the agency; (2) identifies incident reporting requirements, including timelines and required data elements, inspection provisions, and post-incident activities; and (3) requires certification of sanitization of government and government-activity-related files and information. Additionally, new clause 3052.204-7Y, *Notification and Credit Monitoring Requirements for Personally Identifiable Information Incidents*, requires contractors to have in place procedures and the capability to notify and provide credit monitoring services to any individual whose PII or SPII was under the control of the contractor or resided in the information system at the time of the incident.

These measures are necessary because of the urgent need to protect CUI and respond appropriately when DHS contractors experience incidents with DHS information. Persistent and pervasive high-profile breaches of Federal information continue to demonstrate the need to ensure that information security protections are clearly, effectively, and consistently addressed in contracts. This final rule strengthens and expands existing HSAR language to ensure adequate security when contractor and/or

subcontractor employees will have access to CUI; CUI will be collected or maintained on behalf of the agency; or Federal information systems, which include contractor information systems operated on behalf of the agency, are used to collect, process, store, or transmit CUI.

b. Analysis Considerations

In accordance with the regulatory analysis guidance articulated in OMB's Circular A–4 and consistent with DHS's practices in previous rulemakings, this regulatory analysis focuses on the likely consequences of the final rule (i.e., costs and cost savings that accrue to entities affected) relative to the baseline (existing regulations, statutes, and guidance).

This analysis covers 10 years (2023 through 2032) to ensure it captures major costs and cost savings that accrue over time. DHS expresses all quantifiable impacts in 2020 dollars and uses discount rates of 3 and 7 percent, pursuant to Circular A–4.[5] The impacts of this final rule are estimated relative to the existing baseline (i.e., current requirements for security and training for contractors). DHS estimates impacts using a range of potential costs and cost savings to account for uncertainty and, therefore, presents the estimated impacts using a lower bound, upper bound, and primary estimate. The primary estimate is calculated by taking the average of the upper bound and lower bound estimates. DHS was unable to quantify some costs, cost savings, and benefits of the final rule. DHS describes them qualitatively in section IV.A.3 (Subject-by-Subject Analysis).

(1) Analysis Baseline

The final rule primarily codifies and updates the HSAR regulation to clarify, streamline, and include requirements from existing regulations, including those required by:

[5] All present value calculations assume a base year of 2022.

- Existing HSAR 3052.204-70, *Security Requirements for Unclassified Information Technology Requirements*
- 32 CFR Part 2002, *Controlled Unclassified Information (CUI)*
- Federal Information Security Modernization Act of 2014 (44 U.S.C. 3551)
- NIST SP 800–53, *Recommended Security and Privacy Controls for Federal Information Systems and Organizations*, and NIST SP 800-88, *Guidelines for Media Sanitization* (Appendix G)

A more comprehensive discussion of existing requirements is in section IV.A.3 (Subject-by-Subject Analysis). In addition, the prior Exhibit 2 maps provisions of the final rule to relevant existing requirements.

The analysis of this final rule estimates impacts relative to a baseline assuming no regulatory action. The baseline represents the agency's best assessment of what the world would be like absent this action. A key difference in the impacts estimated in this final rule compared to the proposed rule is that the proposed rule did not perform an analysis incremental to a baseline of existing regulations. Instead, the proposed rule presented estimates of the costs of activities covered by provisions, regardless of whether those activities were new requirements from the rulemaking. In particular, two of the larger cost estimates (FTE oversight and continuous monitoring) presented in the proposed rule were for activities already required by existing regulations and are discussed below.

(a) Baseline cost of continuous monitoring

Alternate I to clause 3052.204-7X, *Authority to Operate*, mandates that contractors operating Federal information systems comply with information system continuous monitoring requirements. FISMA regulations (44 U.S.C. 3551, et seq.) already require continuous monitoring and vendors therefore historically have incurred costs associated with continuous monitoring equipment and labor costs for setup,

maintenance, and operation of continuous monitoring.[6] Consistent with the proposed rule analysis, internal DHS data and cost information from vendors indicate the cost for vendors complying with continuous monitoring requirements to acquire continuous monitoring equipment ranges from a lower bound of $82,034 to an upper bound of $376,107, with a primary estimate of $229,071.[7] ATO vendors already are required by FISMA to incur this one-time cost.

ATO vendors that are complying with continuous monitoring requirements also have labor in place to operate information systems and perform continuous monitoring. Internal DHS historical data and cost information from vendors indicate that labor costs for initial setup and operation of information systems to perform continuous monitoring range from a lower bound of $50,506 to an upper bound of $69,848 per year, with a primary estimate of $59,827.[8] This labor cost occurs every 3 years when there is ATO renewal and systems need to be initialized. ATO vendors complying with existing continuous monitoring requirements also have an annual cost to maintain systems that assist with continuous monitoring. DHS estimates this cost ranges from a lower bound of $6,448 to an upper bound of $19,343, with a primary estimate of $12,895.[9]

(b) Baseline cost of FTE oversight

Meeting the requirements of the final rule requires overseeing compliance of individuals who have received security authorization, as already required by FISMA. The final rule maintains this requirement in Alternate I to clause 3052.204-7X, *Authority to*

---

[6] *See* 44 U.S.C. 3551.

[7] The final rule estimates of obtaining continuous monitoring equipment are consistent with the proposed rule (Safeguarding of Controlled Unclassified Information (HSAR Case 2015–001) [Docket No. DHS–2017–0006]) estimates and adjusted to 2020 dollars from 2016 dollars using the GDP deflator (Bureau of Economic Analysis (BEA) NAIPA Table 1.1.9 Implicit Price Deflators for Gross Domestic Product: *https://apps.bea.gov/iTable/iTable.cfm?reqid=19&step=2#reqid=19&step=2&isuri=1&1921=survey*).

[8] Estimates were developed using cost information from multiple vendors whose contracts with DHS include similar continuous monitoring requirements. The final rule estimates of labor cost to perform continuous monitoring are consistent with the proposed rule estimates and adjusted to 2020 dollars using the GDP deflator.

[9] The final rule estimates of labor cost to maintain systems that assist with continuous monitoring are consistent with the proposed rule estimates and adjusted to 2020 dollars using the GDP deflator.

Operate. The costs associated with this FTE oversight stem directly from a vendor's pre-existing information security posture. Vendors, particularly those operating in the IT space, have been complying with these requirements for years. In these instances, the vendors have the existing infrastructure (i.e., hardware, software, and personnel) to implement these requirements and implementation costs are lower. The same is also true for many vendors that provide professional services to the Government and use IT to provide those services. Alternatively, vendors with less experience and capability in this area procure the hardware and software necessary to implement these requirements, as well as the labor costs associated with personnel needed to implement and oversee these requirements. Costs vary depending on the hardware and software selected and the skill set each contractor requires in its employee(s) responsible for ensuring compliance with these requirements.

DHS determined the costs associated with FTE oversight of the final rule requirements by requesting cost information from multiple vendors. These data indicated that the cost of FTE oversight ranges from a lower bound of $69,848 to an upper bound of $348,168, with a primary estimate of $209,008.[10] These costs decline as vendors become more sophisticated and efficient.

(2) Estimated Number of Vendors Impacted by the Final Rule

The final rule will apply to DHS contractors that require access to CUI, collect or maintain CUI on behalf of the Government, or operate Federal information systems, which include contractor information systems operated on behalf of the agency that collect, process, store, or transmit CUI. DHS estimated the number of vendors subject to the final rule using FY 2019 and FY 2020 Federal Procurement Data System (FPDS) data on unique vendors awarded contracts under the most likely applicable Product and

[10] The final rule estimates of FTE oversight are consistent with the proposed rule estimates and adjusted to 2020 dollars using the GDP deflator.

Service Codes (PSCs) in FY 2019 and FY 2020. FPDS data indicated that 3,030 unique vendors were awarded contracts under the most likely applicable PSCs in FY 2019 and 3,203 in FY 2020, including small business. However, not all contractors will be subject to clause 3052.204-7X, *Safeguarding of Controlled Unclassified Information*.

(a) Population of Alternate I to clause 3052.204-7X,

Safeguarding of Controlled Unclassified Information

DHS estimated that approximately 5.5 percent of the unique vendors identified as being awarded contracts under the most likely applicable PSCs in FY 2019 and FY 2020 would be subject to the requirements of Alternate I to clause 3052.204-7X, *Safeguarding of Controlled Unclassified Information*, and will be required to respond to ATO requirements and submit SA documentation.[11] DHS calculated the number of vendors subject to Alternate I to clause 3052.204-7X, *Authority to Operate*, by multiplying the number of unique vendors awarded contracts under the most likely applicable PSCs in FY 2019 (3,030 unique vendors) and FY 2020 (3,203 unique vendors) by 5.5 percent. DHS estimated that in FY 2019, 167 vendors would be subject to Alternate I to clause 3052.204-7X,[12] and in FY 2020, 176 vendors would be subject to Alternate I to clause 3052.204-7X.[13] DHS then took a 2-year average of the 167 and 176 figures to estimate

---

[11] The estimate of the number of entities to which the rule will apply was established by reviewing FPDS data for FY 2019 and FY 2020, internal DHS contract data, experience with similar safeguarding requirements used in certain DHS contracts, and the most likely applicable PSCs. Additionally, the estimate was reviewed and validated by the cognizant departmental subject-matter experts (SMEs) for information security, information system security, and privacy. These SMEs have extensive experience in the requirements of these clauses and their applicability and current implementation in DHS contracts. The data review identified 3,030 unique contractors that were awarded contracts under the most likely applicable PSCs in FY 2019 and 3,203 in FY 2020, including small and large businesses. However, not all contractors awarded contracts under the most likely applicable PSCs are subject to clauses 3052.204-7X, *Safeguarding of Controlled Unclassified Information*, and 3052.204-7Y, *Notification and Credit Monitoring Requirements for Personally Identifiable Information Incidents*. A number of factors determine the applicability of the clauses, and a case-by-case analysis of each action is required to determine the applicability of the clauses. Further, the clauses are delineated by those entities that are granted access to CUI but information systems will not be used to process, store, or transmit CUI, and those that are required to meet the ATO requirements because Federal information systems will be used to process, store, or transmit CUI.

[12] Calculation: 3,030 unique vendors subject to Alternate I to clause 3052.204-7X in FY 2019 * 5.5 percent of PSCs affected by the rule = 166.65 vendors.

[13] Calculation: 3,203 unique vendors subject to Alternate I to clause 3052.204-7X in FY 2020 * 5.5 percent of PSCs affected by the rule = 176.16 vendors.

that approximately 171 vendors will be subject to Alternate I to clause 3052.204-7X.[14] DHS presents the ATO population estimate in Exhibit 3 along with the population estimate used in the NPRM.

Exhibit 3: Change to ATO Population Compared to NPRM		
Component	**NPRM**	**Final Rule**
ATO vendors subject to the rule	137	171

(b) Population of paragraphs (b), (c), (d), (e), and (f) of clause 3052.204-7X, *Safeguarding of Controlled Unclassified Information*

Based on FY 2019 and FY 2020 data, DHS estimated that approximately 11 percent of the unique vendors identified as being awarded contracts under the most likely applicable PSCs in FY 2019 and FY 2020 would be subject to the requirements of paragraphs (b), (c), (d), (e), and (f) of clause 3052.204-7X, *Safeguarding of Controlled Unclassified Information*.[15] DHS calculated the number of vendors subject to paragraphs (b), (c), (d), (e), and (f) by multiplying the number of unique vendors awarded contracts under the most likely applicable PSCs in FY 2019 (3,030 unique vendors) and FY 2020 (3,203 unique vendors) by 11 percent. DHS estimated that in FY 2019, 333 vendors would be subject to paragraphs (b), (c), (d), (e), and (f),[16] and in FY 2020, 352 vendors would be subject to paragraphs (b), (c), (d), (e), and (f).[17] DHS then took a 2-year average of the 333 and 352 figures to estimate that approximately 343 vendors will be subject to

[14] Calculation: (166.65 vendors subject to Alternate I to clause 3052.204-7X in FY 2019 + 176.16 vendors subject to Alternate I to clause 3052.204-7X in FY 2020) / 2 = 171.4 vendors (the 2-year average number of vendors subject to Alternate I to clause 3052.204-7X).

[15] The estimate of the number of entities to which the rule will apply was established by reviewing FPDS data for FY 2019 and FY 2020, internal DHS contract data, experience with similar safeguarding requirements used in certain DHS contracts, and the most likely applicable PSCs. Additionally, the estimate was reviewed and validated by the cognizant departmental SMEs for information security, information system security, and privacy. See footnote 11 for more detail.

[16] Calculation: 3,030 unique vendors subject to paragraphs (b), (c), (d), (e), and (f) in FY 2019 * 11 percent of PSCs affected by the rule = 333.3 vendors.

[17] Calculation: 3,203 unique vendors subject to paragraphs (b), (c), (d), (e), and (f) in FY 2019 * 11 percent of PSCs affected by the rule = 352.33 vendors.

paragraphs (b), (c), (d), (e), and (f).[18] DHS presents the non-ATO population estimates in Exhibit 4 along with the non-ATO population estimates used in the NPRM.

Exhibit 4: Changes to non-ATO Population Compared to NPRM		
Component	**NPRM**	**Final Rule**
Non-ATO prime contractors subject to the rule	274	343
Non-ATO subcontractors subject to the rule	411	514

(3) Changes to Component Costs Relative to NPRM

Under the proposed rule, DHS requested cost information from vendors whose contracts with DHS include requirements similar to this final rule; obtained cost input from FedRAMP, for which DHS is a participant; reviewed the Congressional Budget Office Cost Estimate for the Personal Data Protection and Breach Accountability Act of 2011; reviewed pricing from the Identity Protection Services (IPS) blanket purchase agreements recently awarded by the General Services Administration (GSA); and reviewed internal price data from DHS's Managed Compliance Services and notification and credit monitoring services contracts. DHS determined that the majority of these costs are unchanged from the proposed rule and, therefore, adjusts them to 2020 dollars.[19] For two costs, DHS obtained updated estimates: the cost of notification of incidents to individuals whose PII was compromised and the cost of credit monitoring services. These costs are discussed in more detail in the subject-by-subject analysis. For this final rule analysis, DHS presents a low, high, and primary estimate to capture uncertainty in the costs to affected entities. Exhibit 5 summarizes the costs in the NPRM and this final rule.

Exhibit 5: Summary of Changes to Component Costs[t]

	NPRM**		Final Rule		
Component Cost	**Low**	**High**	**Low**	**Primary**	**High**
Independent assessment ($ per entity)	$123,615	$150,000	$132,836*	$147,012*	$161,189*
Equipment to set up continuous monitoring system ($ per entity)	$76,340	$350,000	$82,034*	$229,071*	$376,107*
Labor to perform continuous monitoring ($ per entity)	$47,000	$65,000	$50,506*	$59,827*	$69,848*
Maintain continuous monitoring equipment ($ per entity)	$6,000	$18,000	$6,448*	$12,895*	$19,343*

[18] Calculation: (333.30 vendors subject to paragraphs (b), (c), (d), (e), and (f) in FY 2019 + 352.33 vendors subject to paragraphs (b), (c), (d), (e), and (f) in FY 2020) / 2 = 342.82 vendors (the 2-year average number of vendors subject to paragraphs (b), (c), (d), (e), and (f)).

[19] The values used in the NPRM adjusted to 2020 dollars using a GDP deflator of 105.736 for 2016 and a GDP deflator of 113.623 for 2020. Bureau of Economic Analysis: Table 1.1.4. Price Indexes for GDP. *https://apps.bea.gov/iTable/iTable.cfm?reqid=19&step=2#reqid=19&step=2&isuri=1&1921=survey*.

FTE oversight ($ per entity)	$65,000	$324,000	$69,848*	$209,008*	$348,168*
Reporting an incident to DHS ($ per incident)	$500	$1,500	$537*	$1,075*	$1,612*
Notification of incident to individuals ($ per impacted individual)	$1.03	$4.60	$0.84	$2.72	$4.60
Credit monitoring services ($ per impacted individual)	$60	$260	$4.16	$6.53	$8.90

[t] The table includes costs that were presented in the proposed rule that are considered baseline costs in the final rule, including continuous monitoring and FTE oversight.
* Value is unchanged but is inflated to 2020 dollars.
** The proposed rule did not use a primary estimate.

3. Subject-by-Subject Analysis

DHS's analysis below covers the estimated costs and cost savings of the final rule relative to the existing baseline. DHS emphasizes that many of the provisions in the final rule are existing requirements in the statute, regulations, or regulatory guidance and presents existing requirements related to each provision in the previous Exhibit 2. The final rule codifies these practices under one set of rules; therefore, they are not considered "new" burdens resulting from the final rule. This rule addresses the safeguarding requirements specified in:

- FISMA, which (1) provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets; (2) recognizes the highly networked nature of the current Federal computing environment and provides effective governmentwide management and oversight of the related information security risks, including coordination of information security efforts throughout the civilian, national security, and law enforcement communities; (3) provides for development and maintenance of minimum controls required to protect Federal information and information systems; and (4) provides a mechanism for improved oversight of Federal agency information security programs, including through automated security tools to continuously diagnose and improve security.
- NIST SP 800–53, *Recommended Security and Privacy Controls for Federal Information Systems and Organizations*, and NIST SP 800–88, *Guidelines for Media Sanitization* (Appendix G). Pursuant to FISMA, NIST is responsible for

developing information security standards and guidelines, including minimum requirements for Federal information systems (Note: Such standards and guidelines do not apply to national security systems without the express approval of appropriate Federal officials exercising policy authority over such systems.). NIST SP 800–53 sets forth information security requirements contractors operating a Federal information system must meet prior to collecting, processing, storing, or transmitting CUI in that information system. NIST SP 800–88 assists organizations and system owners in making practical sanitization decisions based on the categorization of confidentiality of their information.

- OMB Circular A–130, *Managing Information as a Strategic Resource*, which establishes general policy for the planning, budgeting, governance, acquisition, and management of Federal information, personnel, equipment, funds, IT resources, and supporting infrastructure and services. The Circular's appendices include responsibilities for protecting Federal information resources and managing PII.
- OMB Memorandum M–17–12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, which sets forth the policy for Federal agencies to prepare for and respond to a breach of PII, including a framework for assessing and mitigating the risk of harm to individuals potentially affected by a breach, as well as guidance on whether and how to provide notification and services to those individuals.
- OMB Memorandum M–20–04, *Fiscal Year 2019–2020 Guidance on Federal Information Security and Privacy Management Requirements*, which in accordance with FISMA provides agencies with FY 2020 reporting guidance and deadlines.

- E.O. 13556, *Controlled Unclassified Information*, and its implementing regulation at 32 CFR part 2002, which defines the executive branch's CUI Program and establishes policy for designating, handling, and decontrolling information that qualifies as CUI and standardizes the way the executive branch handles information that requires protection under laws, regulations, or Governmentwide policies but that does not qualify as classified information.

DHS considered both the costs and benefits associated with the requirements of clause 3052.204-7X, *Safeguarding of Controlled Unclassified Information*, and clause 3052.204-7Y, *Notification and Credit Monitoring Requirements for Personally Identifiable Information Incidents*, specifically those requirements believed to be of most import to industry, such as the requirements to: obtain an independent assessment, perform continuous monitoring, report all known and suspected incidents, provide notification and credit monitoring services in the event an incident impacts PII, document sanitization of Government and Government-activity-related files and information, as well as ensure overall compliance with the requirements of the clauses. Accordingly, the regulatory analysis focuses on the costs and cost savings that can be attributed exclusively to the new requirements in the final rule.

The analysis assumes that not all efforts (e.g., retrieving and retaining records) are attributed solely to this new rule; only those actions resulting from this rule that are not customary to normal business practices are attributed to this estimate. There are several instances of requirements of the final rule that are not new requirements; for example, the analysis does not include revisions to clause 3052.204-71, *Contractor Employee Access*, as the revisions to this clause are primarily clarifying in nature (i.e., updates to terminology). Regarding the training requirements discussed in the revisions to this clause, specifically additional training that may be required due to the CUI Specified status of the information, this requirement is not new for DHS contractors. CUI Basic and

CUI Specified categories of information previously were considered sensitive but unclassified information under prior Departmental policy. When additional training is required for CUI Specified information, it is because the statute or regulation for that specific category requires certain training. DHS and its contractors always complied with the additional training requirements when they were applicable under its sensitive but unclassified information policy. As such, these requirements are covered by the existing information collection that covers this clause (i.e., OMB Control Number 1600–0003). Another example is clause 3052.204-7X(c)(3), specifying contractors and subcontractors should not include CUI in the body of any email but instead include such information in encrypted attachments, with passwords to these files sent via separate emails. The cost of this requirement (i.e., the time to compose two emails, rather than one email) is not quantified because it is an existing requirement. Other requirements are required by existing regulations. For example, FISMA requires continuous monitoring and vendors therefore historically have incurred costs associated with continuous monitoring equipment and labor costs for setup, maintenance, and operation of continuous monitoring. The previous Exhibit 2 lays out which provisions have requirements that already exist under FISMA, existing HSAR, and other regulations.

a. Costs

This section quantifies the costs associated with the final rule changes, including costs associated with rule familiarization, reporting and recordkeeping requirements, conducting an independent assessment, and security review. DHS presents each cost with an associated lower bound estimate, upper bound estimate, and primary estimate.

(1) Quantitative Costs

(a) Rule Familiarization

When the final rule takes effect, ATO vendors will need to familiarize themselves with the new regulations. Consequently, this imposes a one-time cost on ATO vendors in

the first year of the rule. DHS estimates the time to review the rule is 1 hour. Therefore, DHS estimated the one-time cost of rule familiarization to be $12,590.[20] DHS estimated the total cost of rule familiarization over the 10-year period is $12,223 and $11,766 at discount rates of 3 percent and 7 percent, respectively. The annualized cost over the 10-year period is $1,433 and $1,675 at discount rates of 3 percent and 7 percent, respectively.

(b) Reporting and Recordkeeping

DHS has determined that 343 non-ATO vendors and 514 non-ATO subcontractors, for a total of 857 entities (Exhibit 4), are subject to reporting requirements associated with notification and credit monitoring. DHS estimates that each non-ATO vendor will require 36 hours to meet the reporting requirements. Therefore, DHS estimated the cost of reporting for non-ATO vendors to be $2.27 million annually.[21] DHS has determined that 171 ATO vendors are subject to reporting requirements associated with notification and credit monitoring. DHS estimated that each ATO vendor will require 120 hours to meet the reporting requirements. Therefore, DHS estimated that the cost of reporting for ATO vendors is $1.51 million annually.[22]

It is estimated that the number of recordkeepers associated with these clauses (ATO and non-ATO vendors) is 1,028. Both ATO and non-ATO vendors will require the same preparation time and maintenance per response, which is estimated to average 16

---

[20] Calculation: 171.41 ATO vendors * $73.45 loaded hourly wage rate of Information Security Analysts = $12,589.95 one-time, undiscounted cost of rule familiarization to ATO vendors.

[21] Calculation: 857.04 total annual responses * 36 estimated hours per response = 30,852.44 total estimated burden hours. Calculation: 30,852.44 total estimated hours * ($51.72/hour * 1.42 loaded wage rate factor) = $2,266,191. The average hourly salary is based on the hourly wage of private sector information security analysts (*https://www.bls.gov/oes/current/oes151212.htm*). The loaded wage rate factor is based on BLS' estimates for private industry workers by occupational and industry group (*https://www.bls.gov/news.release/ecec.t04.htm*).

[22] Calculation: 171.41 total annual responses * 120 estimated hours per response = 20,569.20 total estimated burden hours. Calculation: 20,569.20 total estimated hours * ($51.72/hour * 1.42 loaded wage rate factor) = $1,510,794.

hours per year, meaning that the total annual recordkeeping burden is 16,455.20 hours.[23] DHS estimates the cost of recordkeeping requirements to be $1.21 million annually.[24]

Finally, the Government will face costs to receive, review, and take action on reporting and recordkeeping submissions. To estimate the cost of receiving, reviewing, and taking action on reporting and recordkeeping submissions, the Department assumed an Information Security Analyst reviews submissions.[25] [26] DHS estimated that the Government's cost of receiving, reviewing, and taking action from incident reporting, incident response activities, PII and SPII notification requirements, credit monitoring, and receipt of certification of sanitization of government and government-activity-related files and information from non-ATO vendors is $452,516 annually.[27] The Government's cost of these activities from ATO vendors is $678,774 annually.[28]

Reporting and recordkeeping requirements impose costs on ATO vendors, non-ATO vendors, and the Government. The total cost of reporting and recordkeeping associated with the final rule is $6.12 million.[29] DHS estimates the total cost of reporting and recordkeeping over the 10-year period is $52.18 million and $42.96 million at discount rates of 3 percent and 7 percent, respectively. The annualized cost estimate over the 10-year period is $6.30 million and $6.55 million at discount rates of 3 percent and 7 percent, respectively.

---

[23] Calculation: 1,028.45 recordkeepers * 16 hours per recordkeeper per year = 16,455.20 hours.
[24] Calculation: 16,455.20 annual reporting hours * ($51.72/hour * 1.42 loaded wage rate factor) hourly wage plus overhead = $1,208,635.
[25] Calculation: $36.64 Private Industry Workers' Total Compensation / $25.80 Private Industry Workers' Wages and Salaries = 1.42 Loaded Wage Factor. Employer Costs for Employee Compensation for private industry workers by occupational and industry group. *https://www.bls.gov/news.release/ecec.t04.htm*.
[26] Loaded hourly wage is $73.45. Calculation: $51.72 * Loaded Wage Factor (1.42). Occupational Employment and Wages, May 2020, Information Security Analyst, *https://www.bls.gov/oes/2020/may/oes151212.htm*.
[27] Calculation: 857.04 non-ATO vendors * 8 hours of review time * $66 hourly wage plus overhead = $452,516. The average hourly salary is based on the OPM GS-13/Step 4 salary ($48.09 an hour) plus a 36.25 percent fringe and overhead burden rate, the one mandated by OMB Memorandum M-08-13 for use in public-private competition, rounded to the nearest dollar, or $66 an hour. Reference Salary Table 2020-RUS, Effective January 2020, found at *https://www.opm.gov*.
[28] Calculation: 171.41 ATO vendors * 60 hours of review time * $66 hourly wage plus overhead = $678,774.
[29] Calculation: $3,776,986 total reporting cost + $1,208,635 recordkeeping cost + $1,131,290 cost to the Government = $6,116,911.

(c) Independent Assessment

According to the changes in Alternate I to clause 3052.204-7X, *Authority to Operate*, contractors must have an independent third party validate the security and privacy controls in place for the information system(s); review and analyze the SA package; and report on technical, operational, and management level deficiencies.[30] The contractor must address all deficiencies before submitting the SA package to the COR for review.

Alternate I to clause 3052.204-7X, *Authority to Operate*, requires ATO vendors to acquire an independent assessment. The independent assessment is used to validate the security and privacy controls in place for the information system prior to submission of the SA package to the Government for review and acceptance. DHS estimated the cost of an independent assessment to ATO vendors by first determining the price of an independent assessment. DHS estimated that the cost of an independent assessment ranges from a lower bound of $132,836 to an upper bound of $161,189, with a primary estimate of $147,012.[31] Once an ATO is accepted and signed by the Government, it is valid for 3 years and must be renewed at that time unless otherwise specified in the ATO letter. As a result, ATO vendors will incur the cost of obtaining an independent assessment in the first year of the study period and in 3-year increments following the initial independent assessment. DHS then determined that 171 ATO vendors are subject to the provision. DHS estimates the total cost of independent assessments over the 10-year period, using the primary estimate, is $71.28 million and $86.09 million at discount rates of 3 percent and 7 percent, respectively. The primary annualized cost estimate over

---

[30] These standards are outlined in NIST SP 800–53, *Security and Privacy Controls for Information Systems and Organizations*, or successor publication, accessible at *https://csrc.nist.gov/publications/sp*.

[31] The $132,836 estimate of an independent assessment is consistent with the proposed rule estimate of $123,615 and adjusted to 2020 dollars using the GDP deflator. The $123,615 estimate of an independent assessment was sourced from cost information requested from multiple vendors whose contracts with DHS require an independent assessment as part of the SA process. The $161,189 estimate of an independent assessment is consistent with the proposed rule estimate of $150,000, which was sourced from FedRAMP data and adjusted to 2020 dollars.

the 10-year period is $10.09 million and $10.15 million at discount rates of 3 percent and 7 percent, respectively. Exhibit 6 summarizes the range of cost estimates of independent assessments.

Exhibit 6: Estimated Monetized Costs of Independent Assessments ($2020 Millions)			
	Cost (Low Estimate)	**Cost (Primary Estimate)**	**Cost (High Estimate)**
10-Year Total (Undiscounted)	$91.08	$100.80	$110.52
10-Year Total (3% Discounted)	$77.79	$86.09	$94.40
10-Year Total (7% Discounted)	$64.40	$71.28	$78.15
Annualized (3% Discounted)	$9.12	$10.09	$11.07
Annualized (7% Discounted)	$9.17	$10.15	$11.13

(d) Security Review

The Government may elect to conduct periodic reviews to ensure that the security requirements contained in contracts are being implemented and enforced. The Government, at its sole discretion, may obtain assistance from other Federal agencies and/or third-party firms to aid in security review activities. Under this requirement, the contractor must afford DHS, the Office of the Inspector General, other government organizations, and contractors working in support of the Government access to the contractor's facilities, installations, operations, documentation, databases, networks, systems, and personnel used in the performance of the contract. The contractor must, through the Contracting Officer and COR, contact the Component or Headquarters CIO, or designee, to coordinate and participate in review and inspection activity by government organizations external to DHS. Access must be provided, to the extent necessary as determined by the Government (including providing all requested images), for the Government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability, and confidentiality of government data or the function of computer systems used in performance of the contract and to preserve evidence of computer crime.

These requirements impose a cost to the contractor to perform the security review and to DHS to review and assist the security review. DHS has determined that it will conduct 50 self-assessment surveys and 4 full assessments annually, which take 3 and 40 hours, respectively. To estimate the cost of receiving, reviewing, and taking action on reporting and recordkeeping submissions, the Department assumed an Information Security Analyst reviews submissions.[32] [33] After completing security reviews, DHS has a GS–13 level analyst review 20 self-assessments and 2 full assessments annually. The total cost to contractors over 10 years to conduct self-assessments and full assessments is $227,696.[34] The total cost to DHS to review self-assessments and full assessments over 10 years is $118,800.[35] The total cost of security review associated with the final rule is $346,496.[36] DHS estimates the total cost of security reviews over the 10-year period—both the self-assessments and full assessments as well as their review—using the primary estimate, is $295,568 and $243,365 at discount rates of 3 percent and 7 percent, respectively. The primary annualized cost estimate over the 10-year period is $34,650 at discount rates of both 3 percent and 7 percent.

(2) Qualitative Costs

DHS is unable to quantify some costs related to clause 3052.204-7X paragraph (c), *Incident Reporting Requirements*, and clause 3052.204-7Y paragraphs (b), *PII and SPII Notification Requirements*, and (c), *Credit Monitoring Requirements*. Monetization is not possible for clause 3052.204-7Y paragraphs (b) and (c) because DHS does not

---

[32] Calculation: $36.64 Private Industry Workers' Total Compensation / $25.80 Private Industry Workers' Wages and Salaries = 1.42 Loaded Wage Factor. Employer Costs for Employee Compensation for private industry workers by occupational and industry group. *https://www.bls.gov/news.release/ecec.t04.htm*.
[33] Loaded hourly wage is $73.45. Calculation: $51.72 * Loaded Wage Factor (1.42). Occupational Employment and Wages, May 2020, Information Security Analyst, *https://www.bls.gov/oes/2020/may/oes151212.htm*.
[34] Calculation: ($73.45 loaded hourly wage * 50 self-assessments * 3 hours per self-assessment) + ($73.45 loaded hourly wage * 4 full assessments * 40 hours per full assessment) = $227,696.
[35] Calculation: ($66 loaded hourly wage * 50 self-assessments * 2 hours review per self-assessment) + ($66 loaded hourly wage * 4 full assessments * 20 hours review per full assessment) = $118,800.
[36] Calculation: $227,696 cost of self-assessments and full assessments + $118,800 cost of reviewing self-assessments and full assessments = $346,496.

track data on the number of individuals whose data are compromised under a data breach. Without this estimate, DHS is unable to determine the average number of individuals whom vendors would have to notify and who will require credit monitoring services. DHS anticipates a cost to vendors that are subject to the requirements of clause 3052.204-7Y paragraphs (b) and (c) and experience a data breach.

(a) Costs related to clause 3052.204-7X, *Safeguarding of Controlled Unclassified Information*, paragraph (c), *Incident Reporting Requirements*

Clause 3052.204-7X, *Safeguarding of Controlled Unclassified Information*, paragraph (c), *Incident Reporting Requirements*, requires contractors to report known or suspected incidents that involve PII or SPII within 1 hour of discovery as well as all other incidents (such as those impacting any other category of CUI) within 8 hours of discovery. Contractors must also provide as many of the following data elements that are available at the time the incident is reported, with any remaining data elements provided within 24 hours of submission of the initial incident report:

(i) Unique Entity Identifier (UEI);

(ii) Contract numbers affected unless all contracts by the company are affected;

(iii) Facility CAGE code if the location of the event is different than the prime contractor location;

(iv) Point of contact (POC) if different than the POC recorded in the System for Award Management (address, position, telephone, and email);

(v) Contracting Officer POC (address, telephone, and email);

(vi) Contract clearance level;

(vii) Name of subcontractor and CAGE code if this was an incident on a subcontractor network;

(viii) Government programs, platforms, or systems involved;

(ix) Location(s) of incident;

(x) Date and time the incident was discovered;

(xi) Server names where CUI resided at the time of the incident, both at the contractor and subcontractor level;

(xii) Description of the Government PII or SPII contained within the system; and

(xiii) Any additional information relevant to the incident.

DHS determined the cost of reporting an incident by requesting cost information from multiple vendors whose contracts with DHS include similar incident reporting requirements and reviewing internal historical data. These data indicated that the cost of reporting an incident to DHS ranges from a lower bound of $537 per incident to an upper bound of $1,612 per incident, with a primary estimate of $1,075 per incident.[37] DHS cannot quantify the aggregate total of these costs because DHS does not track the origin of security event notices and is therefore unable to determine how many security event notices external contractors reported to their respective Component SOC or the DHS Network Operations Security Center.

(b) Costs related to clause 3052.204-7Y, *Safeguarding of Controlled Unclassified Information*, paragraph (b), *PII and SPII Notification Requirements*

Clause 3052.204-7Y, *Safeguarding of Controlled Unclassified Information*, paragraph (b), *PII and SPII Notification Requirements*, sets forth the notification procedures and capability requirements for contractors when notifying any individual whose PII and/or SPII was under the control of the contractor or resided in the information system at the time of the incident. The provision requires that, when appropriate, vendors must provide notification to individuals affected by the incident.

[37] The final rule estimates of incident reporting are consistent with the proposed rule and adjusted to 2020 dollars using the GDP deflator.

In response to compromised PII/SPII, the Government determines whether notification is appropriate, thereby adding another cost to both non-ATO and ATO vendors. DHS obtained values for the cost of providing notification to individuals via the GSA Data Breach Response and Identity Protection Services web page.[38] The Department assumed that vendors will purchase the "Per Impacted Individual" package (as opposed to the "Per Enrollee" package) when obtaining notification services.[39] The Department collected per impacted individual data from Experian, Identity Theft Guards, and Sontiq and then determined the lowest value and highest value for each service to create the following estimates. DHS estimated that the cost of notifying each individual ranges from $0.84 ($0.29 plus $0.55 for a standard-sized letter stamp) to $4.60 per year per individual, or $2.72 on average, depending on the level of security, features, and data included in each plan by the companies providing these services.

DHS cannot quantify an aggregate total of this cost due to the rule because DHS does not track at the Department level the number of notifications required on either an annual or per-incident basis. Additionally, the number of individuals requiring notification varies from incident to incident. Because DHS cannot estimate the number of individuals who require notification on an annual or per-incident basis, the Department cannot quantify an aggregate total of this cost due to the rule. Finally, there are existing State or local laws requiring notification and DHS does not collect data on where breaches are occurring. Therefore, DHS does not collect data on the baseline notification costs that already exist. The bearer of the notification cost—the government or the contractor—is determined on a case-by-case basis based on DHS's discretion.

---

[38] GSA eLibrary Data Breach and Identity Protection: *https://www.gsaelibrary.gsa.gov/ElibMain/sinDetails.do?scheduleNumber=MAS&specialItemNumber=541990IPS&executeQuery=YES*.

[39] Per Impacted Individual pricing is used when the enrollment rate of a breach is unknown and services are therefore provided to the entire impacted population regardless of enrollment status.

(c) Costs related to clause 3052.204-7Y, *Safeguarding of Controlled Unclassified Information*, paragraph (c), *Credit Monitoring Requirements*

Clause 3052.204-7Y, *Safeguarding of Controlled Unclassified Information*, paragraph (c), *Credit Monitoring Requirements*, requires that contractors, in the event of an incident, provide credit monitoring services, including call center services, if directed by the Contracting Officer, to any individual whose PII or SPII was under the control of the contractor, or resided in the information system, at the time of the incident for a period beginning the date of the incident and extending not less than 18 months from the date the individual is notified.

This rule requires contractors to provide credit monitoring services (including call center services) to any individual whose PII or SPII resided in a compromised information system. DHS updated costs estimated in the proposed rule by obtaining values for the cost of providing credit monitoring services to individuals from data on the GSA Data Breach Response and Identity Protection Services web page.[40] The Department assumed that vendors will purchase the "Per Impacted Individual" package (as opposed to the "Per Enrollee" packages) when obtaining credit monitoring services. The Department collected per impacted individual data from Experian, Identity Theft Guards, and Sontiq and then determined the lowest value and highest value for each service to create the following estimates. The Department estimates that the cost of private credit monitoring services ranges from $4.16 to $8.90 per year per individual, or $6.53 on average, depending on the level of security, features, and data included in each plan by the companies providing these services. The Department assumes that vendors will have the capabilities to obtain favorable credit monitoring prices. DHS cannot

[40] GSA eLibrary Data Breach and Identity Protection: *https://www.gsaelibrary.gsa.gov/ElibMain/sinDetails.do?scheduleNumber=MAS&specialItemNumber=541990IPS&executeQuery=YES.*

quantify these costs because it does not have estimates for the population of individuals affected.

(3) Summary of Costs

The changes in the final rule are expected to incur a cost to vendors that are subject to the final rule requirements. DHS estimates the 10-year costs to range from an undiscounted lower bound of $152.60 million to an undiscounted upper bound of $172.04 million. Over the 10-year analysis period, DHS estimates that the final rule will incur a total lower bound cost to vendors of $130.28 million at a 3-percent discount rate and $107.62 million at a 7-percent discount rate. DHS estimates that over the 10-year analysis period, the final rule will incur a total upper bound cost to vendors of $146.88 million at a 3-percent discount rate and $121.376 million at a 7-percent discount rate. Exhibit 7 provides a summary of the total estimated costs due to the final rule by provision.

Exhibit 7: Estimated 10-Year Monetized Costs the Final Rule by Provision ($2020 millions)

Provision	Cost (Low Estimate)	Cost (Primary Estimate)	Cost (High Estimate)
Independent assessment	$91.08	$100.80	$110.52
Rule familiarization	$0.01	$0.01	$0.01
Reporting and Recordkeeping	$61.17	$61.17	$61.17
Security Review	$0.35	$0.35	$0.35
10-Year Undiscounted Total	$152.60	$162.32	$172.04
10-Year Total with a Discount Rate of 3%	$130.28	$138.58	$146.889
10-Year Total with a Discount Rate of 7%	$107.62	$114.49	$121.37

b. Qualitative Cost Savings

This section describes the cost savings associated with the final rule changes, including cost savings associated with clause 3052.204-7X paragraph (b), *Handling of Controlled Unclassified Information*, and Alternate I to clause 3052.204-7X, *Authority to Operate*.

The final rule will result in multiple cost savings associated with the transparency and consistency provided to contractors considering doing business with DHS. One cost saving is associated with the reduced time for DHS to grant an ATO. If a system is

presented to DHS without the correct SRTM and/or with a poorly developed SA package, it can take up to 6 months to correct the issues and rewrite the SA package. In addition, post-assessment activities can be greatly reduced, as the number and severity of those corrections through POA&Ms required would be significantly reduced. DHS is unable to quantify reductions in time required for the ATO process, but lowering the risk of delays has the potential to produce significant time savings to DHS and impacted contractors.

Another cost savings to DHS results from time saved reviewing and reissuing requests for proposals and finding new contractors when they are unable to implement the SRTM. Under the final rule, contractors are more clearly notified of the system requirements of the contract up front, resulting in more bids from contractors capable of meeting DHS standards. Previously, embedding requirements in separate documents (i.e., Statement of Work, Statement of Objectives, or Performance Work Statement) or through existing clause 3052.204-70, *Security Requirements for Unclassified Information Technology Requirements*, had the following impacts: (1) created inconsistencies in the identification of information security requirements for applicable contracts; (2) required the identification and communication of security controls for which compliance was necessary after contract award had been made; and (3) resulted in delays in contract performance. Under this final rule, DHS is less likely to have to put the project on hold to reissue a request for proposal or look for an alternate contractor, which reduces the reissuance of solicitations in situations where contractors are unable to implement the SRTM. Avoiding the reissuance of proposals also results in cost savings associated with avoiding background investigations for IT contractors, which can range in cost from approximately $425 to $1,000 per investigation. DHS is unable to quantify the cost savings associated with more bids from contractors capable of meeting DHS standards because we are unable to estimate the number of avoided reissuances that will occur.

The final rule will reduce the response time when incidents do occur, resulting in quicker identification of breaches and reducing the severity of incidents, thereby producing significant cost savings. The timely reporting of incidents is critical to prevent the impact of the incident from expanding, ensure incident response and mitigation activities are undertaken quickly, and ensure individuals are timely notified of the possible or actual compromise of their PII and offered credit monitoring services when applicable. Contractors were previously not consistently provided with specific incident reporting timelines, leaving the timeliness of incident reporting to the contractor. Standardizing incident reporting leads to more proactive incident response, potentially faster incident resolution, and potential reduction in the scope and impact of the incident depending on the nature of the attack (i.e., fewer records breached). According to Cyentia Institute's 2020 Information Risk Insights Study report, the median cost of a data breach in the public sector was approximately $132,000, with higher cost cases (95th percentile) reaching approximately $13 million per incident.[41] An alternative source, the most recent (2021) Verizon Data Breach Investigations Report (DBIR), indicates that while 76 percent of the reported data breaches did not result in a loss, the losses for the remaining 24 percent ranged between $148 and $1.6 million, with a median breach cost of $30,000 for 95 percent of the cases with losses.[42] Based on an analysis of 79,000 breaches, the 2021 Verizon DBIR shows that approximately 60 percent of the incidents are discovered in days, while 20 percent could take months or longer to discover.[43] Early detection of the incidents is critical in preventing data loss, data encryption, and other damage.[44]

---

[41] Cyentia Institute, *2020 Information Risk Insights Study* (Mar. 2020), *https://www.cyentia.com/wp-content/uploads/IRIS2020_cyentia.pdf*.
[42] Verizon, *2021 Data Breach Investigations Report* (May 2021), *https://www.verizon.com/business/en-nl/resources/reports/dbir/*.
[43] Based on Verizon DBIR analysis of breaches in 88 countries. *https://enterprise.verizon.com/resources/articles/s/how-to-minimize-your-mean-time-to-detect-a-breach/*.
[44] Michael Paye, "Poor incident detection can cost your organization a fortune" (Sept. 24, 2020), Security Magazine, *https://www.securitymagazine.com/articles/93173-poor-incident-detection-can-cost-your-organization-a-fortune*.

Reducing the time to identify the breach results in immediate short-term benefits, such as improving the effectiveness of incident management, reducing false positives, improving triage by lowering the cost of trivial true positives,[45] minimizing mission disruption and the resulting impact on revenue and performance, and reducing the cost of investigation.[46] There are also significant long-term benefits of early discovery. Specifically, decreasing time to detection enables streamlined incident data collection and reporting, which allows for the generation of actionable insights and advice to the broader Federal Civilian Executive Branch, State-Local-Tribal-Territorial Government, and Critical Infrastructure communities on the proactive measures that reduce the potential for large-scale service disruptions. Cumulatively, short- and long-term benefits increase costs to the adversary, thus reducing the effectiveness of adversary campaigns. However, lacking an authoritative source that establishes a defensible estimate of the difference in a breach cost in the public sector based on the mean time to detection, DHS is unable to estimate the reduction in time to identify a breach under the final rule and, therefore, does not quantify these cost savings and other benefits.

c. Qualitative Benefits

This section describes the benefits associated with the final rule changes, including cost savings associated with clause 3052.204-7X paragraph (d), *Incident Response Requirements*, and clause 3052.204-7Y paragraphs (b), *PII and SPII Notification Requirements*, and (c), *Credit Monitoring Requirements*.

There are several nonquantifiable benefits of the final rule in addition to the cost savings discussed above. One of the main benefits is reducing the severity of a data breach to individuals and businesses that would have data compromised by a data breach.

---

[45] Druce MacFarlane, "The 3 hidden costs of incident response" (May 10, 2018), CSO Online, *https://www.csoonline.com/article/3270940/the-3-hidden-costs-of-incident-response.html*.
[46] Michael Paye, "Poor incident detection can cost your organization a fortune" (Sept. 24, 2020), Security Magazine, *https://www.securitymagazine.com/articles/93173-poor-incident-detection-can-cost-your-organization-a-fortune* and AlertOps, "MTTR vs MTBF vs MTTD vs MTTF" (2021) *https://alertops.com/mttd-vs-mttf-vs-mtbf-vs-mttr/.*

There are four cost categories that contribute to the total cost of a data breach: detection and escalation, lost business, notification, and ex-post response (including credit monitoring, identity protection services, and more). While some costs, such as the cost of lost business due to lowered trust, are not relevant to DHS, DHS expects this rule to reduce other costs, such as notification and ex-post response (credit monitoring and identity protection services). Although there is no way to eliminate the risk of breach completely, the purpose of this rule is to mitigate the negative effects of breaches, which include identity theft.

The public will be better notified of breaches in their data, allowing for better self-monitoring for identity theft. In particular, the rule requires contractors to have in place procedures and capability to notify any individual whose PII and/or SPII was under the control of the contractor or resided in the information system at the time of an incident. At a minimum, this notification must include: a brief description of the incident; a description of the types of PII or SPII involved; a statement as to whether the PII or SPII was encrypted or protected by other means; steps individuals may take to protect themselves; what the contractor and/or the Government are doing to investigate the incident, to mitigate the incident, and to protect against any future incidents; and information identifying who individuals may contact for additional information. DHS is unable to monetize the benefit associated with notifying individuals that their data may be compromised because it is difficult to estimate the number of individuals who may have their data compromised and to monetize the benefit of notification. DHS is unable to monetize the benefit associated with notification because DHS cannot estimate the number of individuals who require notification on an annual or per-incident basis. DHS does not track at the Department level the number of notifications required on either an annual or per-incident basis. Additionally, the number of individuals requiring notification varies from incident to incident. Because DHS cannot estimate the number of

individuals who require notification on either an annual or per-incident basis, the Department cannot monetize the benefit of notification.

The final rule also will produce a benefit to individuals associated with providing credit monitoring services. Under the final rule, when directed by the contracting officer, contractors are required to provide credit monitoring services, including call center services, to any individual whose PII or SPII was under the control of the contractor, or resided in the information system, at the time of the incident for a period beginning on the date of the incident and extending not less than 18 months from the date the individual is notified. Credit monitoring services can be particularly beneficial to the affected public, as they can assist individuals in the early detection of identity theft as well as notify individuals of changes that appear in their credit report, such as creation of new accounts, changes to their existing accounts or personal information, or new inquiries for credit. Such notification affords individuals the opportunity to take steps to minimize any harm associated with unauthorized or fraudulent activity. DHS is unable to quantify the benefit associated with providing credit monitoring services because it is difficult to estimate the number of individuals who may require credit monitoring services.

Another benefit of the *Safeguarding of Controlled Unclassified Information* clause is expedited reporting timelines. Incident reporting requires a contractor to report all known or suspected incidents to the Component SOC, or the DHS Enterprise SOC if the Component SOC is not available, in accordance with *4300A Sensitive Systems Handbook*, Attachment F, *Incident Response*. All known or suspected incidents involving PII or SPII must be reported within 1 hour of discovery. All other incidents must be reported within 8 hours of discovery. Timely reporting of incidents is critical for proactive incident response and potentially faster incident resolution. Also, timely reporting prevents the impact of the incident from expanding, ensures incident response

and mitigation activities are undertaken quickly, and ensures that individuals are timely notified of the possible or actual compromise of their PII and offered credit monitoring services when applicable. DHS is unable to quantify this benefit because it is difficult to quantify the impact of timely reporting on the severity of an incident.

4. Summary

DHS presents the estimated range of costs under the final rule in Exhibit 8. DHS estimates the final rule will have an annualized cost that ranges from $15.32 million to $17.28 million at a discount rate of 7 percent and a total 10-year cost that ranges from $107.62 million to $121.37 million at a discount rate of 7 percent. DHS was unable to quantify the cost savings or benefits associated with the rule. However, the final rule is expected to produce cost savings by reducing the time required to grant an ATO, reducing DHS time reviewing and reissuing proposals because contractors are better qualified, and reducing the time to identify a data breach. The final rule also produces benefits by better notifying the public when their data are compromised, requiring the provision of credit monitoring services so that the public can better monitor and avoid costly consequences of data breaches, and reducing the severity of incidents through timely incident reporting.

Exhibit 8: Estimated Monetized Costs of the Final Rule ($2020 millions)

	Costs		
	Low	**Primary**	**High**
2023	$28.93	$31.63	$33.79
2024	$6.15	$6.15	$6.15
2025	$6.15	$6.15	$6.15
2026	$28.92	$31.35	$33.78
2027	$6.15	$6.15	$6.15
2028	$6.15	$6.15	$6.15
2029	$28.92	$31.35	$33.78
2030	$6.15	$6.15	$6.15
2031	$6.15	$6.15	$6.15
2032	$28.92	$31.35	$33.78
Undiscounted 10-Year Total	$152.60	$162.32	$172.04
10-Year Total with Discount Rate of 3%	$130.28	$138.58	$146.89
10-Year Total with Discount Rate of 7%	$107.62	$114.49	$121.37
Annualized with Discount Rate of 3%	$15.27	$16.25	$17.22
Annualized with Discount Rate of 7%	$15.32	$16.30	$17.28

5. Regulatory Alternatives

DHS evaluated two alternatives to the chosen approach of independent assessment, which requires vendors to obtain an independent assessment from a third party to validate the security and privacy controls in place for an information system prior to submission of the security authorization package to the Government for review and acceptance. In general, when assessing compliance with a standard or set of requirements, there are three alternatives: (1) first-party attestation or self-certification; (2) second-party attestation (i.e., internal independent); or (3) third-party attestation. While the first two options may be considered the least economically burdensome, third-party attestation is an accepted best practice in commercial industry as objectivity increases with independence. DHS has selected the chosen approach of requiring vendors to obtain an independent assessment from a third party to ensure a truly objective measure of an entity's compliance with the requisite security and privacy controls. Recent high-profile breaches of Federal information demonstrate the need for Departments, agencies, and industry to ensure that information security protections are clearly, effectively, and consistently addressed and appropriately implemented in contracts. The benefits of using a third party to perform an independent assessment extends to the contractor, as the contractor can use the results of the independent assessment to demonstrate its cybersecurity excellence for customers other than DHS.

B. Regulatory Flexibility Act

The Regulatory Flexibility Act of 1980, 5 U.S.C. 601 et seq., as amended by the Small Business Regulatory Enforcement Fairness Act of 1996, Pub. L. 104–121 (Mar. 29, 1996), hereafter jointly referred to as the "RFA," requires Federal agencies engaged in rulemaking to assess the impact of regulations that will have a significant economic impact on a substantial number of small entities. The agency also is required to respond

to public comments on the NPRM.[47] The Chief Counsel for Advocacy of the SBA did not submit public comments on the NPRM.

The Department believes that this final rule may have a significant economic impact on a substantial number of small entities. Therefore, the Department publishes this final regulatory flexibility analysis (FRFA) that builds on the assessment provided in the initial regulatory flexibility analysis (IRFA) published as part of the NPRM. The Department invited interested persons to submit comments on impacts to small entities during the proposed rule phase.

1. A statement of the need for, and objectives of, the rule

DHS has determined that the new rulemaking is needed to implement security and privacy measures to safeguard CUI and facilitate improved incident reporting to DHS. The final rule enables DHS more efficiently to identify, remediate, mitigate, and resolve incidents when they occur, not necessarily completely prevent them. DHS understands that there is no "true" way to completely prevent an incident from occurring. However, these measures are intended to decrease the likelihood of occurrence with full knowledge that there is no such thing as an "unhackable" system.

The final rule adds a new clause at 3052.204-7X, *Safeguarding of Controlled Unclassified Information*, that ensures adequate protection of CUI. That new clause: (1) identifies CUI handling requirements and security processes and procedures applicable to Federal information systems, which include contractor information systems operated on behalf of the agency; (2) identifies incident reporting requirements, including timelines and required data elements, inspection provisions, and post-incident activities; and (3) requires certification of sanitization of government and government-activity-related files and information. Additionally, new clause 3052.204-7Y, *Notification and Credit Monitoring Requirements for Personally Identifiable Information Incidents*, requires

[47] *See* 5 U.S.C. 604.

contractors to have in place procedures and the capability to notify and provide credit monitoring services to any individual whose PII or SPII was under the control of the contractor or resided in the information system at the time of the incident.

These measures are necessary because of the urgent need to protect CUI and respond appropriately when DHS contractors experience incidents with DHS information. Persistent and pervasive high-profile breaches of Federal information continue to demonstrate the need to ensure that information security protections are addressed clearly, effectively, and consistently in contracts. This final rule strengthens and expands existing HSAR language to ensure adequate security when contractor and/or subcontractor employees will have access to CUI; CUI will be collected or maintained on behalf of the agency; or Federal information systems, which include contractor information systems operated on behalf of the agency, are used to collect, process, store, or transmit CUI.

2. **A statement of the significant issues raised by the public comments in response to the IRFA, a statement of the assessment of the agency of such issues, and a statement of any changes made to the proposed rule as a result of such comments**

The Department did not receive public comments on the IRFA.

3. **The response of the agency to any comments filed by the Chief Counsel for Advocacy of the SBA in response to the proposed rule, and a detailed statement of any change made to the proposed rule as a result of the comments**

The Department did not receive comments from the Chief Counsel for Advocacy of the SBA.

4. A description of and an estimate of the number of small entities to which the rule will apply or an explanation of why no such estimate is available

a. Definition of *Small Entity*

The RFA defines a "small entity" as a (1) small not-for-profit organization; (2) small governmental jurisdiction; or (3) small business. The Department used the entity size standards defined by SBA, in effect as of August 19, 2019, to classify businesses as small.[48] SBA establishes separate standards for individual 6-digit North American Industry Classification System (NAICS) codes, and standard cutoffs typically are based on either the average number of employees or the average annual receipts. For example, small businesses generally are defined as having fewer than 500, 1,000, or 1,250 employees in manufacturing industries and less than $7.5 million in average annual receipts for nonmanufacturing industries. However, some exceptions do exist, the most notable being that depository institutions (including credit unions, commercial banks, and noncommercial banks) are classified by total assets (small defined as less than $550 million in assets). Small governmental jurisdictions are another noteworthy exception. They are defined as the governments of cities, counties, towns, townships, villages, school districts, or special districts with populations of less than 50,000 people.[49]

b. Number of Small Entities

The Department collected employment and annual revenue data from the business information provider Data Axle and merged those data into FY 2020 Federal FPDS data. The FPDS data contained PSC information for each vendor identifying the type of service being provided to DHS. This dataset allowed the Department to identify the number and type of small entities in the FPDS data, and their PSC information, as well as their annual revenues. DHS identified 2,218 unique vendors with PSCs for FY 2020 that

---

[48] SBA *Table of Small Business Size Standards Matched to North American Industry Classification System Codes* (Aug. 2019), *https://www.sba.gov/document/support-table-size-standards*.
[49] *See https://advocacy.sba.gov/resources/the-regulatory-flexibility-act* for details.

may be impacted by the final rule. Of those 2,218 vendors, the Department was able to obtain data matches of revenue or employees for 366 vendors in FY 2020. Duplicate vendors that appeared multiple times within the dataset were removed (i.e., the same vendor appearing multiple times). The Department was unable to obtain data matches for 184 vendors in FY 2020. In order to prevent underestimating the number of small entities the final rule would affect, DHS conservatively considers all the nonmatched vendors as small entities for the purpose of this analysis. Of the 366 vendors with employee or revenue matches, the Department identified 265 unique vendors (or 48 percent of the sample) as small.[50] Within the 265 matched small vendors, the Department was unable to obtain revenue data for four vendors. These data points are displayed in Exhibit 9 below.

Exhibit 9: Number of Small Entities		
Parameter	**Quantity**	**Proportion of Sample (Percent)**
Population	3,203	-
Population (unique entities)	2,218	-
Minimum Required Sample	328	-
Selected Sample	550	100%
Nonmatched Sample Segment	184	33%
Matched Sample Segment	366	67%
Matched Small Entities	265	48%
Sub-Sample Missing Revenue Data	4	2%
Matched Non-Small Entities	101	18%
Number of Small Entities Discovered in Research	**449**	**82%**

In sum, the Department classified 449 vendors as small.[51] Of these unique small entities, 261 of them had revenue data available from Data Axle. The Department's analysis of the financial impact of this final rule on small entities is based on the number of small unique entities with revenue data (261).

To provide clarity on the industries impacted by this regulation, Exhibit 10 shows the number of unique small entities (265) in FY 2020 within each NAICS code at the 6-digit and 4-digit level.

Exhibit 10: Number of Small Entities by NAICS Code

[50] SBA *Table of Small Business Size Standards Matched to North American Industry Classification System Codes*. (Aug. 2019), *https://www.sba.gov/document/support-table-size-standards*.
[51] Calculation: 184 nonmatched entities + 265 matched entities = 449 small entities.

6-Digit NAICS	Description	Number of Small Employers	Percent of Small Employers
541511	Custom Computer Programming Services	21	8%
443142	Electronics Stores	16	6%
541618	Other Management Consulting Services	11	4%
423610	Electrical Apparatus and Equipment, Wiring Supplies, and Related Equipment Merchant Wholesalers	10	4%
511210	Software Publishers20	10	4%
541614	Process, Physical Distribution and Logistics Consulting Services	8	3%
541330	Engineering Services	7	3%
561990	All Other Support Services	7	3%
238990	All Other Specialty Trade Contractors	6	2%
561621	Security Systems Services (except Locksmiths)	6	2%
Other NAICS		163	61%
4-Digit NAICS	**Description**	**Number of Small Employers**	**Percent of Small Employers**
5416	Management, Scientific, and Technical Consulting Services	27	10%
5415	Computer Systems Design and Related Services	26	10%
4431	Electronics and Appliance Stores	16	6%
4236	Household Appliances and Electrical and Electronic Goods Merchant Wholesalers	11	4%
5413	Architectural, Engineering, and Related Services	10	4%
5616	Investigation and Security Services	10	4%
5112	Software Publishers	10	4%
2389	Other Specialty Trade Contractors	7	3%
5619	Other Support Services	7	3%
5419	Other Professional, Scientific, and Technical Services	7	3%
Other NAICS		134	49%

A small percentage of entities in the sample segment are educational institutions or not-for-profit entities.[52] Using data with the profit/non-profit status of each vendor in the sample segment, we count the number of for-profit and not-for-profit entities and the number of small and non-small entities.[53] We assume that all unspecified entities—those marked as neither educational institutions, non-profit organizations, or for-profit

[52] Educational institutions include HBCUs, private universities or colleges, State-controlled institutions of higher learning, Tribal colleges, veterinary colleges, or other educational institutions.
[53] The SBA's Office of Advocacy defines small organizations as not-for-profit entities that are independently owned and operated and not dominant in their field. For more information, visit *https://www.sba.gov/sites/default/files/advocacy/How-to-Comply-with-the-RFA-WEB.pdf*.

organizations—are for-profit businesses. Table 11 includes these data for both entities we were able to match and non-matched entities.

Exhibit 11: Number of Small Entities

Parameter	Quantity	Proportion of Sample (Percent)
Selected Sample	550	100.0
Profit	496	90.2
Non-Profit	19	3.4
Educational Institution	6	1.1
Other	29	5.3

c. Projected Impacts to Affected Small Entities

The Department has estimated the incremental costs for small entities from the baseline (i.e., the 2017 proposed rule) to this final rule. We estimated the costs of obtaining an independent assessment and rule familiarization. Although the sample population of small entities identified in this analysis is 449, DHS does not anticipate the actual number of small entities impacted by the final rule to be of this magnitude. As discussed in the E.O. 12866 section, DHS expects 171 entities to be impacted by cost provisions annually. The Department anticipates these 171 entities would have a distribution of large and small entities, and impacts to the small entities, that follow the sample population's distribution of size and costs presented in this FRFA.

Small entities in the IT field will be subject to only the independent assessment, ongoing maintenance of continuous monitoring, and rule familiarization costs. DHS classified an entity as being in the IT field if their PSC began with a "7" or "D," or if the PSC matched any of the following codes: 5810, 6350, AJ11, AJ21, AJ23, AJ43, R423, R430, R431, R611, and R615. Additionally, entities classified as non-ATO will be subject to only rule familiarization costs. DHS classified an entity as being non-ATO if their PSC and description was as follows: (1) S201 - Housekeeping - Custodial Janitorial; (2) 6515 - Medical and Surgical Instruments, Equipment, and Supplies; (3) S216 - Housekeeping - Facilities Operations Support; (4) R614 - Support - Administrative: Paper Shredding; or (5) U008 - Education/Training - Training/Curriculum Development.

The estimates included in this analysis are consistent with those presented in the E.O. 12866 section and include costs of rule familiarization, reporting and recordkeeping, and independent assessment.

The Department presents the impacts of the final rule on small entities as a percent of revenue in Exhibit 12 below.

Exhibit 12: Summary of Small Entity Costs as a Percent of Revenue

	50 Percent			75 Percent			90 Percent		
Impacts	**# of small entities**	% of small entities	Cumulative %	**# of small entities**	% of small entities	Cumulative %	**# of small entities**	% of small entities	Cumulative %
<1%	**39**	15%	15%	**34**	13%	13%	**29**	11%	11%
1-5%	**83**	31%	46%	**82**	31%	44%	**86**	33%	44%
5-10%	**48**	18%	64%	**47**	18%	62%	**42**	16%	59%
10-25%	**58**	22%	86%	**59**	22%	84%	**59**	22%	82%
25-50%	**23**	9%	95%	**27**	10%	94%	**26**	10%	92%
>50%	**13**	5%	100%	**15**	6%	100%	**22**	8%	100%
Total	**264**			**264**			**264**		

DHS expects its contractors may choose to reflect these costs in the price and cost proposals they submit to the Department. Therefore, the Department conducted a sensitivity analysis with varying levels of passthrough assumed for small businesses. DHS does not assume a specific percentage of costs that vendors will pass on since some vendors may choose to pass on fewer costs in pursuance of a competitive advantage on their price. Therefore, the Department presents three scenarios using the primary estimates of the rule costs: (1) vendors pass on 50 percent of rule costs to the Department; (2) vendors pass on 75 percent of rule costs to the Department; and (3) vendors pass on 90 percent of rule costs to the Department. The results of the sensitivity analysis are displayed in Exhibit 13 below.

Exhibit 13: Sensitivity of Small Entity Costs Assuming Different Passthroughs

	50 Percent			75 Percent			90 Percent		
Impacts	**# of small entities**	% of small entities	Cumulative %	**# of small entities**	% of small entities	Cumulative %	**# of small entities**	% of small entities	Cumulative %
<1%	**70**	27%	27%	**109**	41%	41%	**157**	59%	59%
1–5%	**100**	38%	64%	**99**	38%	79%	**85**	32%	92%
5–10%	**43**	16%	81%	**32**	12%	91%	**14**	5%	97%
10–25%	**38**	14%	95%	**19**	7%	98%	**8**	3%	100%

25–50%	**8**	3%	98%	**5**	2%	100%	**0**	0%	100%
>50%	**5**	2%	100%	**0**	0%	100%	**0**	0%	100%
Total	**264**			**264**			**264**		

5. A description of the projected reporting, recordkeeping, and other compliance requirements of the rule, including an estimate of the classes of small entities that will be subject to the requirement and the type of professional skills necessary for preparation of the report or record

The final rule has reporting and recordkeeping requirements impacting small entities. DHS needs information required by clauses 3052.204-7X, *Safeguarding of Controlled Unclassified Information*, and 3052.204-7Y, *Notification and Credit Monitoring Requirements for Personally Identifiable Information Incidents*, to implement the requirements for safeguarding against unauthorized contractor/subcontractor disclosure and inappropriate use of CUI that contractors and subcontractors may have access to during the course of contract performance. Reporting and recordkeeping for the SA package consists of the following: Security Plan, Contingency Plan, Contingency Plan Test Results, Configuration Management Plan, Security Assessment Plan, Security Assessment Report, and Authorization to Operate Letter. Additional documents that may be required include a Plan(s) of Action and Milestones and Interconnection Security Agreement(s). Additional requirements include an independent assessment, security review, renewal of the ATO (required every 3 years unless stated otherwise), and Federal reporting and continuous monitoring requirements.

6. **A description of the steps the agency has taken to minimize the significant economic impact on small entities consistent with the stated objectives of applicable statutes, including a statement of the factual, policy, and legal reasons for selecting the alternative adopted in the final rule and why each of the other significant alternatives to the rule considered by the agency that affects the impact on small entities was rejected**

The Department considered alternative requirements for independent assessment that would be less burdensome on small entities. In general, when assessing compliance with a standard or set of requirements, there are three alternatives: (1) first-party attestation or self-certification; (2) second-party attestation (i.e., internal independent); or (3) third-party attestation. While the first two options may be considered the least economically burdensome, third-party attestation is an accepted best practice in commercial industry as objectivity increases with independence. DHS has selected the chosen approach of requiring vendors to obtain an independent assessment from a third party to ensure a truly objective measure of an entity's compliance with the requisite security and privacy controls. Recent high-profile breaches of Federal information demonstrate the need for Departments, agencies, and industry to ensure that information security protections are clearly, effectively, and consistently addressed and appropriately implemented in contracts. The benefits of using a third party to perform an independent assessment extends to the contractor, as the contractor can use the results of the independent assessment to demonstrate its cybersecurity excellence for customers other than DHS.

The information security requirements associated with this rule are not geared toward a type of contractor; the requirements are based on the sensitivity of the information and the impact on the program, the Government, and security in the event CUI is breached. That standard would not vary based on the size of the entity. DHS has

determined that the costs associated with compliance with the security requirements of this rule are a necessary expense to ensure DHS CUI is adequately protected and to produce the resulting benefits and cost savings that accrue to DHS, vendors, and the public from the provisions of the final rule, as discussed in the E.O. 12866 section.

C. Paperwork Reduction Act

The Paperwork Reduction Act (44 U.S.C. ch. 35) applies. The rule contains information collection requirements. Accordingly, DHS will be submitting a request for approval of a new information collection requirement concerning this rule to OMB under 44 U.S.C. 3501, et seq.

The collection requirements for this rule are based on two new clauses, 3052.204-7X, *Safeguarding of Controlled Unclassified Information*, and 3052.204-7Y, *Notification and Credit Monitoring Requirements for Personally Identifiable Information Incidents*.

Overview of Information Collection:

(1) *Type of Information Collection:* New Collection.

(2) *Title of the Form/Collection:* Homeland Security Acquisition Regulation: Safeguarding of Controlled Unclassified Information.

(3) *Agency form number, if any, and the applicable component of DHS sponsoring the collection:* No form; OCPO.

(4) *Affected public who will be asked or required to respond; as well as a brief abstract*: The affected public is business or other for-profit institutions. DHS needs the information required by clauses 3052.204-7X and 3052.204-7Y to implement the requirements for safeguarding against unauthorized contractor/subcontractor disclosure and inappropriate use of CUI that contractors and subcontractors may have access to during the course of contract performance. Responses are required for respondents to obtain or retain benefits.

(5) *An estimate of the total number of respondents and the amount of time estimated for an average respondent to respond*: The estimated number of respondents for reporting is 1,028. The weighted average public reporting burden for this collection of information is estimated to be approximately 50 hours per response to comply with the requirements, including time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. This weighted average is based on an estimated 36 hours per response to comply with the requirements when an ATO is not required and an estimated 120 hours to comply with the requirements when an ATO is required (i.e., when a contractor is required to submit an SA package).[54] The SA package consists of the following: Security Plan, Contingency Plan, Contingency Plan Test Results, Configuration Management Plan, Security Assessment Plan, Security Assessment Report, and Authorization to Operate Letter. Additional documents that may be required include a Plan(s) of Action and Milestones and Interconnection Security Agreement(s). Additional requirements include an independent assessment, security review, renewal of the ATO (required every 3 years unless stated otherwise), and Federal reporting and continuous monitoring requirements. It is estimated that the number of recordkeepers associated with these clauses will be 1,028 and the estimated burden per response is 16 hours.

(6) *An estimate of the total public burden (in hours) associated with the information collection:* The total estimated annual hour burden associated with this collection is 67,820.

(7) *An estimate of the total public burden (in cost) associated with the information collection:* The estimated total annual cost burden associated with this collection of information is $4,476,120.

List of Subjects

[54] Estimated hours weighted by 171 ATO vendors and 857 non-ATO vendors.

48 CFR Parts 3001, 3002, 3004, and 3052

Government procurement.

For reasons set out in the preamble, DHS amends chapter 30 of title 48 of the Code of Federal Regulations as set forth below.

1. The authority citation for 48 CFR parts 3001, 3002, 3004, and 3052 is revised to read as follows:

Authority: 5 U.S.C. 301–302, 41 U.S.C. 1707, 41 U.S.C. 1702, 41 U.S.C. 1303(a)(2), 48 CFR part 1, subpart 1.3, and DHS Delegation Number 0702.

PART 3001—FEDERAL ACQUISITION REGULATIONS SYSTEM

2. In section 3001.106 amend paragraph (a) by adding a new OMB control number at the end of the list to read as follows:

3001.106 OMB Approval under the Paperwork Reduction Act.

(a) * * *

OMB Control No. 1601–0023 (Safeguarding of Controlled Unclassified Information)

* * * * *

PART 3002–DEFINITIONS OF WORDS AND TERMS

3. Amend section 3002.101 by adding the definitions “Adequate security”, “Controlled unclassified information (CUI)”, “Federal information”, “Federal information system”, “Handling”, “Information resources”, “Information security”, and “Information systems” to read as follows:

Adequate security means security protections commensurate with the risk resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information. This includes ensuring that information hosted on behalf of an agency and information systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability protections through the application of cost-effective security controls.

* * * * *

Controlled unclassified information (CUI) is any information the Government creates or possesses, or an entity creates or possesses for or on behalf of the Government (other than classified information) that a law, regulation, or Governmentwide policy requires or permits an agency to handle using safeguarding or dissemination controls. This definition includes the following CUI categories and subcategories of information:

(1) Chemical-terrorism Vulnerability Information (CVI) as defined in 6 CFR part 27, "Chemical Facility Anti-Terrorism Standards," and as further described in supplementary guidance issued by an authorized official of the Department of Homeland Security (including the Revised Procedural Manual "Safeguarding Information Designated as Chemical-Terrorism Vulnerability Information" dated September 2008);

(2) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (title XXII, subtitle B of the Homeland Security Act of 2002 as amended through Pub. L. 116–283), PCII's implementing regulations (6 CFR part 29), the PCII Program Procedures Manual, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security, the PCII Program Manager, or a PCII Program Manager Designee;

(3) Sensitive Security Information (SSI) as defined in 49 CFR part 1520, "Protection of Sensitive Security Information," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or designee), including Department of Homeland Security MD 11056.1, "Sensitive Security Information (SSI)" and, within the Transportation Security Administration, TSA MD 2810.1, "SSI Program";

(4) Homeland Security Agreement Information means information the Department of Homeland Security receives pursuant to an agreement with State, local,

Tribal, territorial, or private sector partners that is required to be protected by that agreement. The Department receives this information in furtherance of the missions of the Department, including, but not limited to, support of the Fusion Center Initiative and activities for cyber information sharing consistent with the Cybersecurity Information Sharing Act of 2015;

(5) Homeland Security Enforcement Information means unclassified information of a sensitive nature lawfully created, possessed, or transmitted by the Department of Homeland Security in furtherance of its immigration, customs, and other civil and criminal enforcement missions, the unauthorized disclosure of which could adversely impact the mission of the Department;

(6) International Agreement Information means information the Department of Homeland Security receives that is required to be protected by an information sharing agreement or arrangement with a foreign government, an international organization of governments or any element thereof, an international or foreign public or judicial body, or an international or foreign private or non-governmental organization;

(7) Information Systems Vulnerability Information (ISVI) means:

(i) Department of Homeland Security information technology (IT) systems data revealing infrastructure used for servers, desktops, and networks; applications name, version, and release; switching, router, and gateway information; interconnections and access methods; and mission or business use/need. Examples of ISVI are systems inventories and enterprise architecture models. Information pertaining to national security systems and eligible for classification under Executive Order 13526 will be classified as appropriate; and/or

(ii) Information regarding developing or current technology, the release of which could hinder the objectives of the Department, compromise a technological advantage or countermeasure, cause a denial of service, or provide an adversary with sufficient

information to clone, counterfeit, or circumvent a process or system;

(8) Operations Security Information means Department of Homeland Security information that could be collected, analyzed, and exploited by a foreign adversary to identify intentions, capabilities, operations, and vulnerabilities that threaten operational security for the missions of the Department;

(9) Personnel Security Information means information that could result in physical risk to Department of Homeland Security personnel or other individuals whom the Department is responsible for protecting;

(10) Physical Security Information means reviews or reports illustrating or disclosing facility infrastructure or security vulnerabilities related to the protection of Federal buildings, grounds, or property. For example, threat assessments, system security plans, contingency plans, risk management plans, business impact analysis studies, and certification and accreditation documentation;

(11) Privacy Information includes both Personally Identifiable Information (PII) and Sensitive Personally Identifiable Information (SPII). PII refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual; and SPII is a subset of PII that if lost, compromised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. To determine whether information is PII, DHS will perform an assessment of the specific risk that an individual can be identified using the information with other information that is linked or linkable to the individual. In performing this assessment, it is important to recognize that information that is not PII can become PII whenever additional information becomes available, in any medium or from any source, that would make it possible to identify an individual. Certain data elements are particularly sensitive and may alone present an increased risk of harm to the individual.

(i) Examples of stand-alone PII that are particularly sensitive include: Social Security numbers (SSNs), driver's license or State identification numbers, Alien Registration Numbers (A-numbers), financial account numbers, and biometric identifiers.

(ii) Multiple pieces of information may present an increased risk of harm to the individual when combined, posing an increased risk of harm to the individual. SPII may also consist of any grouping of information that contains an individual's name or other unique identifier plus one or more of the following elements:

(A) Truncated SSN (such as last 4 digits);

(B) Date of birth (month, day, and year);

(C) Citizenship or immigration status;

(D) Ethnic or religious affiliation;

(E) Sexual orientation;

(F) Criminal history;

(G) Medical information; and

(H) System authentication information, such as mother's birth name, account passwords, or personal identification numbers (PINs).

(iii) Other PII that may present an increased risk of harm to the individual depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. The context includes the purpose for which the PII was collected, maintained, and used. This assessment is critical because the same information in different contexts can reveal additional information about the impacted individual.

* * * * *

Federal information means information created, collected, processed, maintained, disseminated, disclosed, or disposed of by or for the Federal Government, in any medium or form.

Federal information system means an information system used or operated by an agency or by a Contractor of an agency or by another organization on behalf of an agency.

Handling means any use of controlled unclassified information, including but not limited to marking, safeguarding, transporting, disseminating, re-using, and disposing of the information.

* * * * *

Information resources means information and related resources, such as personnel, equipment, funds, and information technology.

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—

(1) Integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;

(2) Confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

(3) Availability, which means ensuring timely and reliable access to and use of information.

Information system means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

* * * * *

PART 3004–ADMINISTRATIVE MATTERS

4. Revise subpart 3004.4 to read as follows:

Subpart 3004.4 Safeguarding Classified and Controlled Unclassified Information within Industry

3004.470 Security requirements for access to unclassified facilities, information resources, and controlled unclassified information.

3004.470-1 Scope.

This section implements DHS policies for assuring adequate security of unclassified facilities, information resources, and controlled unclassified information (CUI) during the acquisition lifecycle.

3004.470-2 Definitions.

As used in this subpart—

Incident means an occurrence that—

(1) Actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or

(2) Constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

3004.470-3 Policy.

(a) DHS requires that CUI be safeguarded when it resides on DHS-owned and operated information systems, DHS-owned and contractor-operated information systems, contractor-owned and/or operated information systems operating on behalf of the Department, and any situation where contractor and/or subcontractor employees may have access to CUI because of their relationship with DHS. There are several Department policies and procedures (accessible at *https://www.dhs.gov/dhs-security-and-training-*

requirements-contractors) that also address the safeguarding of CUI. Compliance with these policies and procedures, as amended, is required.

(b) DHS requires contractor employees that require recurring access to government facilities or access to CUI to complete such forms as may be necessary for security or other reasons, including the conduct of background investigations to determine fitness. Department policies and procedures that address contractor employee fitness are contained in Instruction Handbook Number 121–01–007, *The Department of Homeland Security Personnel Suitability and Security Program*. Compliance with these policies and procedures, as amended, is required.

3004.470-4 Contract Clauses.

(a) Contracting officers shall insert the basic clause at (HSAR) 48 CFR 3052.204-71, *Contractor Employee Access*, in solicitations and contracts when contractor and/or subcontractor employees require recurring access to government facilities or access to CUI. Contracting officers shall insert the basic clause with its Alternate I for acquisitions requiring contractor access to government information resources. For acquisitions in which contractor and/or subcontractor employees will not have access to government information resources, but the Department has determined contractor and/or subcontractor employee access to CUI or government facilities must be limited to U.S. citizens and lawful permanent residents, the contracting officer shall insert the clause with its Alternate II. Neither the basic clause nor its alternates shall be used unless contractor and/or subcontractor employees will require recurring access to government facilities or access to CUI. Neither the basic clause nor its alternates should ordinarily be used in contracts with educational institutions.

(b)(1) Contracting officers shall insert the clause at (HSAR) 48 CFR 3052.204-72, *Safeguarding of Controlled Unclassified Information*, in solicitations and contracts where:

(i) Contractor and/or subcontractor employees will have access to CUI; or

(ii) CUI will be collected or maintained on behalf of the agency.

(2) Contracting officers shall insert the basic clause with its alternate when Federal information systems, which include contractor information systems operated on behalf of the agency, are used to collect, process, store, or transmit CUI.

(c) Contracting officers shall insert the clause at (HSAR) 48 CFR 3052.204-73, *Notification and Credit Monitoring Requirements for Personally Identifiable Information Incidents*, in solicitations and contracts where contractor and/or subcontractor employees have access to PII.

PART 3052—SOLICITATION PROVISIONS AND CONTRACT CLAUSES

5. Remove and reserve clause 3052.204-70.

6. Revise clause 3052.204-71 to read as follows:

3052.204-71 Contractor employee access.

As prescribed in (HSAR) 48 CFR 3004.470-4(a), insert the following clause with appropriate alternates:

CONTRACTOR EMPLOYEE ACCESS (JULY 2023)

(a) *Controlled Unclassified Information (CUI)* is any information the Government creates or possesses, or an entity creates or possesses for or on behalf of the Government (other than classified information) that a law, regulation, or Governmentwide policy requires or permits an agency to handle using safeguarding or dissemination controls. This definition includes the following CUI categories and subcategories of information:

(1) Chemical-terrorism Vulnerability Information (CVI) as defined in 6 CFR part 27, "Chemical Facility Anti-Terrorism Standards," and as further described in supplementary guidance issued by an authorized official of the Department of Homeland Security (including the Revised Procedural Manual "Safeguarding Information Designated as Chemical-Terrorism Vulnerability Information" dated September 2008);

(2) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (title XXII, subtitle B of the Homeland Security Act of 2002 as amended through Pub. L. 116–283), PCII's implementing regulations (6 CFR part 29), the PCII Program Procedures Manual, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security, the PCII Program Manager, or a PCII Program Manager Designee;

(3) Sensitive Security Information (SSI) as defined in 49 CFR part 1520, "Protection of Sensitive Security Information," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or designee), including Department of Homeland Security MD 11056.1, "Sensitive Security Information (SSI)" and, within the Transportation Security Administration, TSA MD 2810.1, "SSI Program";

(4) Homeland Security Agreement Information means information the Department of Homeland Security receives pursuant to an agreement with State, local, Tribal, territorial, or private sector partners that is required to be protected by that agreement. The Department receives this information in furtherance of the missions of the Department, including, but not limited to, support of the Fusion Center Initiative and activities for cyber information sharing consistent with the Cybersecurity Information Sharing Act of 2015;

(5) Homeland Security Enforcement Information means unclassified information of a sensitive nature lawfully created, possessed, or transmitted by the Department of Homeland Security in furtherance of its immigration, customs, and other civil and criminal enforcement missions, the unauthorized disclosure of which could adversely impact the mission of the Department;

(6) International Agreement Information means information the Department of Homeland Security receives that is required to be protected by an information sharing agreement or arrangement with a foreign government, an international organization of governments or any element thereof, an international or foreign public or judicial body, or an international or foreign private or non-governmental organization;

(7) Information Systems Vulnerability Information (ISVI) means:

(i) Department of Homeland Security information technology (IT) systems data revealing infrastructure used for servers, desktops, and networks; applications name, version, and release; switching, router, and gateway information; interconnections and access methods; and mission or business use/need. Examples of ISVI are systems inventories and enterprise architecture models. Information pertaining to national security systems and eligible for classification under Executive Order 13526 will be classified as appropriate; and/or

(ii) Information regarding developing or current technology, the release of which could hinder the objectives of the Department, compromise a technological advantage or countermeasure, cause a denial of service, or provide an adversary with sufficient information to clone, counterfeit, or circumvent a process or system;

(8) Operations Security Information means Department of Homeland Security information that could be collected, analyzed, and exploited by a foreign adversary to identify intentions, capabilities, operations, and vulnerabilities that threaten operational security for the missions of the Department;

(9) Personnel Security Information means information that could result in physical risk to Department of Homeland Security personnel or other individuals whom the Department is responsible for protecting;

(10) Physical Security Information means reviews or reports illustrating or disclosing facility infrastructure or security vulnerabilities related to the protection of

Federal buildings, grounds, or property. For example, threat assessments, system security plans, contingency plans, risk management plans, business impact analysis studies, and certification and accreditation documentation;

(11) Privacy Information includes both Personally Identifiable Information (PII) and Sensitive Personally Identifiable Information (SPII). PII refers to information that can be used to distinguish or trace an individual's identity, either alone, or when combined with other information that is linked or linkable to a specific individual; and SPII is a subset of PII that if lost, compromised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. To determine whether information is PII, DHS will perform an assessment of the specific risk that an individual can be identified using the information with other information that is linked or linkable to the individual. In performing this assessment, it is important to recognize that information that is not PII can become PII whenever additional information becomes available, in any medium or from any source, that would make it possible to identify an individual. Certain data elements are particularly sensitive and may alone present an increased risk of harm to the individual.

(i) Examples of stand-alone PII that are particularly sensitive include: Social Security numbers (SSNs), driver's license or State identification numbers, Alien Registration Numbers (A-numbers), financial account numbers, and biometric identifiers.

(ii) Multiple pieces of information may present an increased risk of harm to the individual when combined, posing an increased risk of harm to the individual. SPII may also consist of any grouping of information that contains an individual's name or other unique identifier plus one or more of the following elements:

(A) Truncated SSN (such as last 4 digits);

(B) Date of birth (month, day, and year);

(C) Citizenship or immigration status;

(D) Ethnic or religious affiliation;

(E) Sexual orientation;

(F) Criminal history;

(G) Medical information; and

(H) System authentication information, such as mother's birth name, account passwords, or personal identification numbers (PINs).

(iii) Other PII that may present an increased risk of harm to the individual depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. The context includes the purpose for which the PII was collected, maintained, and used. This assessment is critical because the same information in different contexts can reveal additional information about the impacted individual.

(b) *Information Resources* means information and related resources, such as personnel, equipment, funds, and information technology.

(c) Contractor employees working on this contract must complete such forms as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed forms shall be submitted as directed by the Contracting Officer. Upon the Contracting Officer's request, the Contractor's employees shall be fingerprinted or subject to other investigations as required. All Contractor employees requiring recurring access to government facilities or access to CUI or information resources are required to have a favorably adjudicated background investigation prior to commencing work on this contract unless this requirement is waived under Departmental procedures.

(d) The Contracting Officer may require the Contractor to prohibit individuals from working on the contract if the Government deems their initial or continued

employment contrary to the public interest for any reason, including, but not limited to, carelessness, insubordination, incompetence, or security concerns.

(e) Work under this contract may involve access to CUI. The Contractor shall access and use CUI only for the purpose of furnishing advice or assistance directly to the Government in support of the Government's activities, and shall not disclose, orally or in writing, CUI for any other purpose to any person unless authorized in writing by the Contracting Officer. For those Contractor employees authorized to access CUI, the Contractor shall ensure that these persons receive initial and refresher training concerning the protection and disclosure of CUI. Initial training shall be completed within 60 days of contract award and refresher training shall be completed every 2 years thereafter.

(f) The Contractor shall include this clause in all subcontracts at any tier where the subcontractor may have access to government facilities, CUI, or information resources.

(End of clause)

ALTERNATE I (JULY 2023)

When the contract will require Contractor employees to have access to information resources, add the following paragraphs:

(g) Before receiving access to information resources under this contract, the individual must complete a security briefing; additional training for specific categories of CUI, if identified in the contract; and any nondisclosure agreement furnished by DHS. The Contracting Officer's Representative (COR) will arrange the security briefing and any additional training required for specific categories of CUI.

(h) The Contractor shall have access only to those areas of DHS information resources explicitly stated in this contract or approved by the COR in writing as necessary for performance of the work under this contract. Any attempts by Contractor personnel to gain access to any information resources not expressly authorized by the

terms and conditions in this contract, or as approved in writing by the COR, are strictly prohibited. In the event of violation of this provision, DHS will take appropriate actions with regard to the contract and the individual(s) involved.

(i) Contractor access to DHS networks from a remote location is a temporary privilege for mutual convenience while the Contractor performs business for DHS. It is not a right, a guarantee of access, a condition of the contract, or government-furnished equipment (GFE).

(j) Contractor access will be terminated for unauthorized use. The Contractor agrees to hold and save DHS harmless from any unauthorized use and agrees not to request additional time or money under the contract for any delays resulting from unauthorized use or access.

(k) Non-U.S. citizens shall not be authorized to access or assist in the development, operation, management, or maintenance of Department IT systems under the contract, unless a waiver has been granted by the Head of the Component or designee, with the concurrence of both the Department's Chief Security Officer (CSO) and the Chief Information Officer (CIO) or their designees. Within DHS Headquarters, the waiver may be granted only with the approval of both the CSO and the CIO or their designees. In order for a waiver to be granted:

(1) There must be a compelling reason for using this individual as opposed to a U.S. citizen; and

(2) The waiver must be in the best interest of the Government.

(l) Contractors shall identify in their proposals the names and citizenship of all non-U.S. citizens proposed to work under the contract. Any additions or deletions of non-U.S. citizens after contract award shall also be reported to the Contracting Officer.

(End of clause)

ALTERNATE II (JUNE 2006)

* * *

(End of clause)

* * * * *

7. Add section 3052.204-72 to read as follows:

3052.204-72 Safeguarding of Controlled Unclassified Information.

As prescribed in (HSAR) 48 CFR 3004.470-4(b), insert the following clause:

SAFEGUARDING OF CONTROLLED UNCLASSIFIED INFORMATION (JULY 2023)

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

Adequate Security means security protections commensurate with the risk resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information. This includes ensuring that information hosted on behalf of an agency and information systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability protections through the application of cost-effective security controls.

Controlled Unclassified Information (CUI) is any information the Government creates or possesses, or an entity creates or possesses for or on behalf of the Government (other than classified information) that a law, regulation, or Governmentwide policy requires or permits an agency to handle using safeguarding or dissemination controls. This definition includes the following CUI categories and subcategories of information:

(1) Chemical-terrorism Vulnerability Information (CVI) as defined in 6 CFR part 27, "Chemical Facility Anti-Terrorism Standards," and as further described in supplementary guidance issued by an authorized official of the Department of Homeland Security (including the Revised Procedural Manual "Safeguarding Information Designated as Chemical-Terrorism Vulnerability Information" dated September 2008);

(2) Protected Critical Infrastructure Information (PCII) as set out in the Critical

Infrastructure Information Act of 2002 (title XXII, subtitle B of the Homeland Security Act of 2002 as amended through Pub. L. 116–283), PCII's implementing regulations (6 CFR part 29), the PCII Program Procedures Manual, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security, the PCII Program Manager, or a PCII Program Manager Designee;

(3) Sensitive Security Information (SSI) as defined in 49 CFR part 1520, "Protection of Sensitive Security Information," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or designee), including Department of Homeland Security MD 11056.1, "Sensitive Security Information (SSI)" and, within the Transportation Security Administration, TSA MD 2810.1, "SSI Program";

(4) Homeland Security Agreement Information means information the Department of Homeland Security receives pursuant to an agreement with State, local, Tribal, territorial, or private sector partners that is required to be protected by that agreement. The Department receives this information in furtherance of the missions of the Department, including, but not limited to, support of the Fusion Center Initiative and activities for cyber information sharing consistent with the Cybersecurity Information Sharing Act of 2015;

(5) Homeland Security Enforcement Information means unclassified information of a sensitive nature lawfully created, possessed, or transmitted by the Department of Homeland Security in furtherance of its immigration, customs, and other civil and criminal enforcement missions, the unauthorized disclosure of which could adversely impact the mission of the Department;

(6) International Agreement Information means information the Department of Homeland Security receives that is required to be protected by an information sharing

agreement or arrangement with a foreign government, an international organization of governments or any element thereof, an international or foreign public or judicial body, or an international or foreign private or non-governmental organization;

(7) Information Systems Vulnerability Information (ISVI) means:

(i) Department of Homeland Security information technology (IT) systems data revealing infrastructure used for servers, desktops, and networks; applications name, version, and release; switching, router, and gateway information; interconnections and access methods; and mission or business use/need. Examples of ISVI are systems inventories and enterprise architecture models. Information pertaining to national security systems and eligible for classification under Executive Order 13526 will be classified as appropriate; and/or

(ii) Information regarding developing or current technology, the release of which could hinder the objectives of the Department, compromise a technological advantage or countermeasure, cause a denial of service, or provide an adversary with sufficient information to clone, counterfeit, or circumvent a process or system;

(8) Operations Security Information means Department of Homeland Security information that could be collected, analyzed, and exploited by a foreign adversary to identify intentions, capabilities, operations, and vulnerabilities that threaten operational security for the missions of the Department;

(9) Personnel Security Information means information that could result in physical risk to Department of Homeland Security personnel or other individuals whom the Department is responsible for protecting;

(10) Physical Security Information means reviews or reports illustrating or disclosing facility infrastructure or security vulnerabilities related to the protection of Federal buildings, grounds, or property. For example, threat assessments, system security plans, contingency plans, risk management plans, business impact analysis studies, and

certification and accreditation documentation;

(11) Privacy Information includes both Personally Identifiable Information (PII) and Sensitive Personally Identifiable Information (SPII). PII refers to information that can be used to distinguish or trace an individual's identity, either alone, or when combined with other information that is linked or linkable to a specific individual; and SPII is a subset of PII that if lost, compromised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. To determine whether information is PII, the DHS will perform an assessment of the specific risk that an individual can be identified using the information with other information that is linked or linkable to the individual. In performing this assessment, it is important to recognize that information that is not PII can become PII whenever additional information becomes available, in any medium or from any source, that would make it possible to identify an individual. Certain data elements are particularly sensitive and may alone present an increased risk of harm to the individual.

(i) Examples of stand-alone PII that are particularly sensitive include: Social Security numbers (SSNs), driver's license or State identification numbers, Alien Registration Numbers (A-numbers), financial account numbers, and biometric identifiers.

(ii) Multiple pieces of information may present an increased risk of harm to the individual when combined, posing an increased risk of harm to the individual. SPII may also consist of any grouping of information that contains an individual's name or other unique identifier plus one or more of the following elements:

(A) Truncated SSN (such as last 4 digits);

(B) Date of birth (month, day, and year);

(C) Citizenship or immigration status;

(D) Ethnic or religious affiliation;

(E) Sexual orientation;

(F) Criminal history;

(G) Medical information; and

(H) System authentication information, such as mother's birth name, account passwords, or personal identification numbers (PINs).

(iii) Other PII that may present an increased risk of harm to the individual depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. The context includes the purpose for which the PII was collected, maintained, and used. This assessment is critical because the same information in different contexts can reveal additional information about the impacted individual.

Federal information means information created, collected, processed, maintained, disseminated, disclosed, or disposed of by or for the Federal Government, in any medium or form.

Federal information system means an information system used or operated by an agency or by a Contractor of an agency or by another organization on behalf of an agency.

Handling means any use of controlled unclassified information, including but not limited to marking, safeguarding, transporting, disseminating, re-using, storing, capturing, and disposing of the information.

Incident means an occurrence that—

(1) Actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or

(2) Constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

Information Resources means information and related resources, such as personnel, equipment, funds, and information technology.

Information Security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—

(1) Integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;

(2) Confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

(3) Availability, which means ensuring timely and reliable access to and use of information.

Information System means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

(b) *Handling of Controlled Unclassified Information.* (1) Contractors and subcontractors must provide adequate security to protect CUI from unauthorized access and disclosure. Adequate security includes compliance with DHS policies and procedures in effect at the time of contract award. These policies and procedures are accessible at *https://www.dhs.gov/dhs-security-and-training-requirements-contractors*.

(2) The Contractor shall not use or redistribute any CUI handled, collected, processed, stored, or transmitted by the Contractor except as specified in the contract.

(3) The Contractor shall not maintain SPII in its invoicing, billing, and other recordkeeping systems maintained to support financial or other administrative functions. It is acceptable to maintain in these systems the names, titles, and contact information for the Contracting Officer's Representative (COR) or other government personnel associated with the administration of the contract, as needed.

(4) Any government data provided, developed, or obtained under the contract, or otherwise under the control of the Contractor, shall not become part of the bankruptcy estate in the event a Contractor and/or subcontractor enters bankruptcy proceedings.

(c) *Incident Reporting Requirements.* (1) Contractors and subcontractors shall report all known or suspected incidents to the Component Security Operations Center (SOC) in accordance with Attachment F, *Incident Response*, to DHS Policy Directive 4300A *Information Technology System Security Program, Sensitive Systems*. If the Component SOC is not available, the Contractor shall report to the DHS Enterprise SOC. Contact information for the DHS Enterprise SOC is accessible at *https://www.dhs.gov/dhs-security-and-training-requirements-contractors*. Subcontractors are required to notify the prime Contractor that it has reported a known or suspected incident to the Department. Lower tier subcontractors are required to likewise notify their higher tier subcontractor, until the prime contractor is reached. The Contractor shall also notify the Contracting Officer and COR using the contact information identified in the contract. If the report is made by phone, or the email address for the Contracting Officer or COR is not immediately available, the Contractor shall contact the Contracting Officer and COR immediately after reporting to the Component or DHS Enterprise SOC.

(2) All known or suspected incidents involving PII or SPII shall be reported within 1 hour of discovery. All other incidents shall be reported within 8 hours of discovery.

(3) CUI transmitted via email shall be protected by encryption or transmitted within secure communications systems. CUI shall be transmitted using a *FIPS 140-2/140-3 Security Requirements for Cryptographic Modules* validated cryptographic module identified on *https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules*. When this is impractical or unavailable, for Federal information systems only, CUI may be transmitted over regular email channels. When

using regular email channels, Contractors and subcontractors shall not include any CUI in the subject or body of any email. The CUI shall be included as a password-protected attachment with the password provided under separate cover, including as a separate email. Recipients of CUI information will comply with any email restrictions imposed by the originator.

(4) An incident shall not, by itself, be interpreted as evidence that the Contractor or Subcontractor has failed to provide adequate information security safeguards for CUI or has otherwise failed to meet the requirements of the contract.

(5) If an incident involves PII or SPII, in addition to the incident reporting guidelines in Attachment F, *Incident Response*, to DHS Policy Directive 4300A *Information Technology System Security Program, Sensitive Systems*, Contractors shall also provide as many of the following data elements that are available at the time the incident is reported, with any remaining data elements provided within 24 hours of submission of the initial incident report:

(i) Unique Entity Identifier (UEI);

(ii) Contract numbers affected unless all contracts by the company are affected;

(iii) Facility CAGE code if the location of the event is different than the prime Contractor location;

(iv) Point of contact (POC) if different than the POC recorded in the System for Award Management (address, position, telephone, and email);

(v) Contracting Officer POC (address, telephone, and email);

(vi) Contract clearance level;

(vii) Name of subcontractor and CAGE code if this was an incident on a subcontractor network;

(viii) Government programs, platforms, or systems involved;

(ix) Location(s) of incident;

(x) Date and time the incident was discovered;

(xi) Server names where CUI resided at the time of the incident, both at the Contractor and subcontractor level;

(xii) Description of the government PII or SPII contained within the system; and

(xiii) Any additional information relevant to the incident.

(d) *Incident Response Requirements.* (1) All determinations by the Department related to incidents, including response activities, will be made in writing by the Contracting Officer.

(2) The Contractor shall provide full access and cooperation for all activities determined by the Government to be required to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of incidents.

(3) Incident response activities determined to be required by the Government may include, but are not limited to, the following:

(i) Inspections;

(ii) Investigations;

(iii) Forensic reviews;

(iv) Data analyses and processing; and

(v) Revocation of the Authority to Operate (ATO), if applicable.

(4) The Contractor shall immediately preserve and protect images of known affected information systems and all available monitoring/packet capture data. The monitoring/packet capture data shall be retained for at least 180 days from submission of the incident report to allow DHS to request the media or decline interest.

(5) The Government, at its sole discretion, may obtain assistance from other Federal agencies and/or third-party firms to aid in incident response activities.

(e) *Certificate of Sanitization of Government and Government-Activity-Related Files and Information.* Upon the conclusion of the contract by expiration, termination, cancellation, or as otherwise indicated in the contract, the Contractor shall return all CUI to DHS and/or destroy it physically and/or logically as identified in the contract unless the contract states that return and/or destruction of CUI is not required. Destruction shall conform to the guidelines for media sanitization contained in NIST SP 800–88, *Guidelines for Media Sanitization*. The Contractor shall certify and confirm the sanitization of all government and government-activity related files and information. The Contractor shall submit the certification to the COR and Contracting Officer following the template provided in NIST SP 800–88, *Guidelines for Media Sanitization*, Appendix G.

(f) *Other Reporting Requirements.* Incident reporting required by this clause in no way rescinds the Contractor's responsibility for other incident reporting pertaining to its unclassified information systems under other clauses that may apply to its contract(s), or as a result of other applicable statutory or regulatory requirements, or other U.S. Government requirements.

(g) *Subcontracts.* The Contractor shall insert this clause in all subcontracts and require subcontractors to include this clause in all lower tier subcontracts when subcontractor employees will have access to CUI; CUI will be collected or maintained on behalf of the agency by a subcontractor; or a subcontractor information system(s) will be used to process, store, or transmit CUI.

(End of clause)

ALTERNATE I (JULY 2023)

When Federal information systems, which include Contractor information systems operated on behalf of the agency, are used to collect, process, store, or transmit CUI, add the following paragraphs:

(h) *Authority to Operate*. The Contractor shall not collect, process, store, or transmit CUI within a Federal information system until an ATO has been granted by the Component or Headquarters CIO, or designee. Once the ATO has been granted by the Government, the Contracting Officer shall incorporate the ATO into the contract as a compliance document. Unless otherwise specified in the ATO letter, the ATO is valid for 3 years. An ATO is granted at the sole discretion of the Government and can be revoked at any time. Contractor receipt of an ATO does not create any contractual right of access or entitlement. The Government's grant of an ATO does not alleviate the Contractor's responsibility to ensure the information system controls are implemented and operating effectively.

(1) *Complete the Security Authorization process.* The Security Authorization (SA) process shall proceed according to DHS Policy Directive 4300A *Information Technology System Security Program, Sensitive Systems* (Version 13.3, February 13, 2023), or any successor publication; and the *Security Authorization Process Guide*, including templates. These policies and templates are accessible at *https://www.dhs.gov/dhs-security-and-training-requirements-contractors*.

(i) *Security Authorization Package*. The SA package shall be developed using the government-provided Security Requirements Traceability Matrix and SA templates. The SA package consists of the following: Security Plan, Contingency Plan, Contingency Plan Test Results, Configuration Management Plan, Security Assessment Plan, Security Assessment Report, and Authorization to Operate Letter. Additional documents that may be required include a Plan(s) of Action and Milestones and Interconnection Security Agreement(s). The Contractor shall submit a signed copy of the SA package, validated by an independent third party, to the COR for review and approval by the Component or Headquarters CIO, or designee, at least 30 days prior to the date of operation of the

information system. The Government is the final authority on the compliance of the SA package and may limit the number of resubmissions of modified documents.

(ii) *Independent Assessment*. Contractors shall have an independent third party validate the security and privacy controls in place for the information system(s). The independent third party shall review and analyze the SA package, and report on technical, operational, and management level deficiencies as outlined in NIST SP 800–53, *Security and Privacy Controls for Information Systems and Organizations*, or successor publication, accessible at *https://csrc.nist.gov/publications/sp*. The Contractor shall address all deficiencies before submitting the SA package to the COR for review.

(2) *Renewal of ATO.* Unless otherwise specified in the ATO letter, the Contractor shall renew the ATO every 3 years. The Contractor is required to update its SA package as part of the ATO renewal process for review and verification of security controls. Review and verification of security controls is independent of the system production date and may include onsite visits that involve physical or logical inspection of the Contractor environment to ensure controls are in place. The updated SA package shall be submitted for review and approval by the Component or Headquarters CIO, or designee, at least 90 days before the ATO expiration date. The Contractor shall update its SA package by one of the following methods:

(i) Updating the SA package in the DHS Information Assurance Compliance System; or

(ii) Submitting the updated SA package directly to the COR.

(3) *Security Review.* The Government may elect to conduct periodic reviews to ensure that the security requirements contained in the contract are being implemented and enforced. The Government, at its sole discretion, may obtain assistance from other Federal agencies and/or third-party firms to aid in security review activities. The Contractor shall afford DHS, the Office of the Inspector General, other government

organizations, and Contractors working in support of the Government access to the Contractor's facilities, installations, operations, documentation, databases, networks, systems, and personnel used in the performance of this contract. The Contractor shall, through the Contracting Officer and COR, contact the Component or Headquarters CIO, or designee, to coordinate and participate in review and inspection activity by government organizations external to DHS. Access shall be provided, to the extent necessary as determined by the Government (including providing all requested images), for the Government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability, and confidentiality of government data or the function of computer systems used in performance of this contract and to preserve evidence of computer crime.

(4) *Federal Reporting and Continuous Monitoring Requirements.* Contractors operating information systems on behalf of the Government shall comply with Federal reporting and information system continuous monitoring requirements. Reporting requirements are determined by the Government and are defined in the Fiscal Year 2015 DHS Information Security Performance Plan, or successor publication, accessible at *https://www.dhs.gov/dhs-security-and-training-requirements-contractors*. The plan is updated on an annual basis. Annual, quarterly, and monthly data collection will be coordinated by the Government. The Contractor shall provide the Government with all information to fully satisfy Federal reporting requirements for information systems. The Contractor shall provide the COR with requested information within 3 business days of receipt of the request. Unless otherwise specified in the contract, monthly continuous monitoring data shall be stored at the Contractor's location for a period not less than 1 year from the date the data are created. The Government may elect to perform information system continuous monitoring and IT security scanning of information systems from government tools and infrastructure.

(End of clause)

8. Add section 3052.204-73 to read as follows:

3052.204-73 Notification and Credit Monitoring Requirements for Personally Identifiable Information Incidents.

As prescribed in (HSAR) 48 CFR 3004.470-4(c), insert the following clause:

3052.204-73 NOTIFICATION AND CREDIT MONITORING REQUIREMENTS FOR PERSONALLY IDENTIFIABLE INFORMATION INCIDENTS (JULY 2023)

(a) *Definitions.* Privacy Information includes both Personally Identifiable Information (PII) and Sensitive Personally Identifiable Information (SPII). PII refers to information that can be used to distinguish or trace an individual's identity, either alone, or when combined with other information that is linked or linkable to a specific individual; and SPII is a subset of PII that if lost, compromised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. To determine whether information is PII, the DHS will perform an assessment of the specific risk that an individual can be identified using the information with other information that is linked or linkable to the individual. In performing this assessment, it is important to recognize that information that is not PII can become PII whenever additional information becomes available, in any medium or from any source, that would make it possible to identify an individual. Certain data elements are particularly sensitive and may alone present an increased risk of harm to the individual.

(1) Examples of stand-alone PII that are particularly sensitive include: Social Security numbers (SSNs), driver's license or State identification numbers, Alien Registration Numbers (A-numbers), financial account numbers, and biometric identifiers.

(2) Multiple pieces of information may present an increased risk of harm to the individual when combined, posing an increased risk of harm to the individual. SPII may also consist of any grouping of information that contains an individual's name or other unique identifier plus one or more of the following elements:

(i) Truncated SSN (such as last 4 digits);

(ii) Date of birth (month, day, and year);

(iii) Citizenship or immigration status;

(iv) Ethnic or religious affiliation;

(v) Sexual orientation;

(vi) Criminal history;

(vii) Medical information; and

(viii) System authentication information, such as mother's birth name, account passwords, or personal identification numbers (PINs).

(3) Other PII that may present an increased risk of harm to the individual depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. The context includes the purpose for which the PII was collected, maintained, and used. This assessment is critical because the same information in different contexts can reveal additional information about the impacted individual.

(b) *PII and SPII Notification Requirements.* (1) No later than 5 business days after being directed by the Contracting Officer, or as otherwise required by applicable law, the Contractor shall notify any individual whose PII or SPII was either under the control of the Contractor or resided in an information system under control of the Contractor at the time the incident occurred. The method and content of any notification by the Contractor shall be coordinated with, and subject to prior written approval by, the Contracting

Officer. The Contractor shall not proceed with notification unless directed in writing by the Contracting Officer.

(2) All determinations by the Department related to notifications to affected individuals and/or Federal agencies and related services (e.g., credit monitoring) will be made in writing by the Contracting Officer.

(3) Subject to government analysis of the incident and direction to the Contractor regarding any resulting notification, the notification method may consist of letters to affected individuals sent by first-class mail, electronic means, or general public notice, as approved by the Government. Notification may require the Contractor's use of address verification and/or address location services. At a minimum, the notification shall include:

(i) A brief description of the incident;

(ii) A description of the types of PII or SPII involved;

(iii) A statement as to whether the PII or SPII was encrypted or protected by other means;

(iv) Steps individuals may take to protect themselves;

(v) What the Contractor and/or the Government are doing to investigate the incident, mitigate the incident, and protect against any future incidents; and

(vi) Information identifying who individuals may contact for additional information.

(c) *Credit Monitoring Requirements.* The Contracting Officer may direct the Contractor to:

(1) Provide notification to affected individuals as described in paragraph (b).

(2) Provide credit monitoring services to individuals whose PII or SPII was under the control of the Contractor or resided in the information system at the time of the incident for a period beginning the date of the incident and extending not less than 18

months from the date the individual is notified. Credit monitoring services shall be provided from a company with which the Contractor has no affiliation. At a minimum, credit monitoring services shall include:

(i) Triple credit bureau monitoring;

(ii) Daily customer service;

(iii) Alerts provided to the individual for changes and fraud; and

(iv) Assistance to the individual with enrollment in the services and the use of fraud alerts.

(3) Establish a dedicated call center. Call center services shall include:

(i) A dedicated telephone number to contact customer service within a fixed period;

(ii) Information necessary for registrants/enrollees to access credit reports and credit scores;

(iii) Weekly reports on call center volume, issue escalation (i.e., those calls that cannot be handled by call center staff and must be resolved by call center management or DHS, as appropriate), and other key metrics;

(iv) Escalation of calls that cannot be handled by call center staff to call center management or DHS, as appropriate;

(v) Customized Frequently Asked Questions, approved in writing by the Contracting Officer in coordination with the Component or Headquarters Privacy Officer; and

(vi) Information for registrants to contact customer service representatives and fraud resolution representatives for credit monitoring assistance.

(End of clause)

9. In section 3052.212-70 amend paragraph (b) of the clause by:

a. Removing "__ 3052.204-70, *Security Requirements for Unclassified Information Technology Resources"*

b. Revising the entry for 3052.204-71, *Contractor Employee Access*, and

c. Adding 3052.204-72, *Safeguarding of Controlled Unclassified Information* and 3052.204-73, *Notification and Credit Monitoring Requirements for Personally Identifiable Information Incidents.*

The revision reads as follows:

3052.212-70 Contract terms and conditions applicable to DHS acquisition of commercial items.

CONTRACT TERMS AND CONDITIONS APPLICABLE TO DHS ACQUISITION OF COMMERCIAL ITEMS (JULY 2023)

* * * * *

(b) * * *

____3052.204-71 Contractor Employee Access.

____Alternate I

____Alternate II

____3052.204-72 Safeguarding of Controlled Unclassified Information.

____3052.204-73 Notification and Credit Monitoring Requirements for Personally Identifiable Information Incidents.

* * * * *

Paul Courtney

Chief Procurement Officer, Department of Homeland Security.

[FR Doc. 2023-11270 Filed: 6/20/2023 8:45 am; Publication Date: 6/21/2023]