DEPARTMENT OF DEFENSE

Defense Acquisition Regulations System

48 CFR Parts 202, 204, 212, 239, and 252

[Docket DARS–2015–0039]

RIN 0750–AI61

Defense Federal Acquisition Regulation Supplement: Network Penetration Reporting and Contracting for Cloud Services (DFARS Case 2013–D018)

AGENCY: Defense Acquisition Regulations System, Department of Defense (DoD).

ACTION: Final rule.

SUMMARY: DoD is adopting as final, with changes, an interim rule amending the Defense Federal Acquisition Regulation Supplement (DFARS) to implement a section of the National Defense Authorization Act for Fiscal Year 2013 and a section of the National Defense Authorization Act for Fiscal Year 2015, both of which require contractor reporting on network penetrations, as well as DoD policy on the purchase of cloud computing services.

DATES: Effective October 21, 2016.

FOR FURTHER INFORMATION CONTACT: Mr. Dustin Pitsch, telephone 571–372–6090.

SUPPLEMENTARY INFORMATION:

I. Background

DoD published two interim rules in the **Federal Register** on August 26, 2015 (80 FR 51739), and December 30, 2015 (80 FR 81472), to implement section 941 of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2013 (Pub. L. 112–239) and section 1632 of the NDAA for FY 2015 (Pub. L. 113–291) regarding contractor reporting of network penetrations, as well as DoD policies and procedures with regard to purchases of cloud computing services. This final rule also implements, for DoD, section 325 of the Intelligence Authorization Act for FY 2014 (Pub. L. 113–126); however, implementing section 325 requires no new changes to the rule, because the reporting requirement is already included.

This rule is part of DoD's retrospective plan, completed in August 2011, under Executive Order 13563, ''Improving Regulation and Regulatory Review.'' DoD's full plan and updates can be accessed at: *http://www.regulations.gov/#!docketDetail;D=DOD-2011-OS-0036.* Twenty-five respondents submitted public comments in response to the interim rules.

II. Discussion and Analysis

DoD reviewed the public comments in the development of the final rule. A discussion of the comments received and the changes made to the rule as a result of those comments follows:

A. Summary of Significant Changes From the Interim Rule

1. The definition of ''covered defense information'' is amended to clarify that, in order to be designated as covered defense information, the information must be controlled technical information or other information (as described in the Controlled Unclassified Information (CUI) Registry) that requires safeguarding or dissemination controls and is (1) marked or otherwise identified in the contract, task order, or delivery order, and provided to the contractor by or on behalf of DoD in connection with the performance of the contract; or (2) collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract. This definition is in line with the National Archives and Record Administration (NARA) ''Controlled Unclassified Information'' final rule published in the **Federal Register** on September 14, 2016 (81 FR 63324). Covered defense information includes all of the categories of information that are considered CUI. The rule also now specifies that all covered contractor information systems need to be protected in accordance with DFARS clause 252.204–7012, Safeguarding Covered Defense Information and Cyber Incident Reporting.

2. The definition of ''covered contractor information system'' is amended to clarify that it is an ''unclassified'' information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information.

3. DFARS 204.7304, Solicitation provision and contract clauses, is amended to specify that DFARS provision 252.204–7008, Compliance with Safeguarding Covered Defense Information Controls, and DFARS clause 252.204–7012 are not prescribed for use in solicitations or contracts that are solely for the acquisition of commercially available off-the-shelf (COTS) items.

4. DFARS 239.7602–1, General, is amended to provide for two exceptions in which a contracting officer may award a contract to acquire cloud services from a cloud service provider (CSP) that has not been granted a provisional authorization by the Defense Information System Agency.

5. DFARS clause 252.204–7000, Disclosure of Information, is amended to clarify that fundamental research, by definition, must not involve any covered defense information.

6. DFARS clause 252.204–7012 is amended to—

a. Specify that contractors are obligated to implement information protection requirements on all covered contractor information systems;

b. Provide additional guidance on requests to vary from National Institute of Standards and Technology (NIST) Special Publication (SP) 800–171, ''Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations;''

c. Clarify that contractors are not required to implement any security requirement if an authorized representative of the DoD Chief Information Officer (CIO) has adjudicated the contractor's request to vary from NIST SP 800–171 and indicated the security requirement to be nonapplicable or to have an alternative, but equally effective, security measure;

d. Require contractors to ensure that external CSPs used in performance of the contract to store, process, or transmit any covered defense information meet security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline (available at *https://www.fedramp.gov/resources/documents/*) and comply with requirements in the clause for cyber incident reporting, malicious software, media preservation and protection, access to additional information and equipment necessary for forensic analysis, and cyber incident damage assessment;

e. Clarify that subcontractor flowdown is only necessary when covered defense information is necessary for performance of the subcontract, and that the contractor may consult with the contracting officer, if necessary, when uncertain if the clause should flow down; and

f. Clarify that the prime contract shall require its subcontractors to notify the prime contractor (or the next higher-tier subcontractor) when submitting requests to vary from a NIST SP 800–171 security requirement to the contracting officer.

B. Analysis of Public Comments

1. Applicability

a. Commercial/COTS Providers

Comment: Multiple respondents commented on the applicability of the rule to contracts and subcontracts for commercial and COTS items. One suggested that the full potential impact of the interim rule on commercial providers should be studied and quantified by DoD before implementation of the rule. Others suggested that the vast majority of commercial contracts do not require that DoD provide information in order for the contractor or subcontractor to perform the work, and that the clause should only apply when DoD provides controlled unclassified information to a contractor as a necessary predicate to performing the contract. One respondent recommended that DoD exempt contracts for commercial and COTS items from application of the final rule or, in the alternative, exempt subcontractors supplying commercial or COTS items from the final rule.

Response: The definition of covered defense information has been amended to clarify, as suggested by the respondents, that in order to be designated as covered defense information, the information must be marked or otherwise identified in the contract and provided to the contractor by or on behalf of DoD in connection with the performance of the contract; or collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract. In addition, to clarify that the rule does not apply to COTS items, the prescriptions at DFARS 204.7304 for use of the provision at 252.204–7008 and the clause at 252.204–7012 are amended to exclude solicitations and contracts solely for the acquisition of COTS items.

b. Fundamental Research

Comment: Several respondents requested clarification regarding the application of the security requirements embedded in DFARS clause 252.204–7012 to fundamental research.

Response: The security requirements in 252.204–7012 need to be in place when covered defense information is present. A contract or project that is appropriately scoped as fundamental research will not contain any covered defense information. The final rule is modified to only flow down the requirements of 252.204–7012 to subcontractors when subcontract performance is for operationally critical support or will involve covered defense information, which means the clause will not flow down to subcontractors that are exclusively performing fundamental research. DFARS clause 252.204–7000 is modified to ensure that it is clear that no covered defense information is involved when making a fundamental research determination.

c. Classified Information System

Comment: One respondent noted that it is unclear whether the clause applies to covered defense information resident on contractor classified information systems. While the covered defense information itself has been explicitly defined as unclassified, covered contractor systems are not specified as such.

Response: The definition for ''covered contractor information system'' has been amended to clarify that it is ''an unclassified information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information.''

d. When Other Security Requirements Apply

Comment: One respondent noted that the mandatory flowdowns of the data security and penetration reporting requirements to health care providers who are subcontractors to military health care plans should be amended to provide that such providers who comply with their data security obligations under Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act are deemed to be in compliance with DoD's data security rules.

Response: If the covered defense information provided is DoD HIPAA, then the requirement would be to meet both HIPAA and NIST SP 800–171. There are requirements of HIPAA that are not in 800–171, just as there are requirements in 800–171 that are not in HIPAA. DFARS 204.7300(b) states that the rule ''does not abrogate any other requirements regarding contractor physical, personnel, information, technical, or general administrative security operations governing the protection of unclassified information.''

e. Small Business

Comment: Several respondents commented on the cost impact to small businesses. One respondent suggested that this rule will impact subcontracting cycles and deliveries throughout the DoD supply chain, due to the inability for smaller suppliers to afford the investment and skilled labor force required to meet and manage these requirements. Multiple respondents requested that, due to the high cost of compliance, DoD provide for an alternative approach for small business. One respondent suggested that DoD consider collaborating with universities or other companies, to provide low-cost cybersecurity services to small businesses, or providing a one-time subsidy to small businesses to help cover the cost of initial consultations with third party vendors. Another suggested that DoD coordinate with the Small Business Administration, Department of Commerce, and other relevant executive agencies, to establish policy, training mechanisms, and learning centers that allow access to the necessary resources to assist small and commercial businesses in creating compliant information systems.

Response: While it is understood that implementing the minimum security controls outlined in the DFARS clause may increase costs, protection of unclassified DoD information is deemed necessary. The cost to the nation in lost intellectual property and lost technological advantage over potential adversaries is much greater than these initial/ongoing investments. The value of the information (and impact of its loss) does not diminish when it moves to contractors (prime or sub, large or small). NIST SP 800–171 was carefully crafted to use performance-based requirements and eliminate unnecessary specificity and include only those security requirements necessary to provide adequate protections for the impact level of CUI (*e.g.,* covered defense information). Implementation of the NIST SP 800–171 security requirements will provide significant benefit to the small business community in the form of increased protection of their intellectual property. In addition, defining one set of standards will help small businesses to avoid a situation in which small business must adopt multiple standards and rule sets as small businesses navigate amongst the many different organizations with which they do business. The addition of a new provision at 252.204–7008, Compliance with Safeguarding Covered Defense Information Controls, ensures that the offeror is aware of the requirements of clause 252.204–7012 and has time to bring their system into compliance and negotiate the terms of the contract accordingly. With regard to training, DoD will engage across both Government and industry to educate and raise awareness of the importance of protecting our controlled unclassified information and to address implementation of the rule.

2. Regulatory Flexibility Act

Comment: Various respondents addressed application of the rule to small entities.

Response: For analysis of applicability to small entities see the regulatory flexibility analysis at section V of this preamble.

3. Definitions

a. Covered Defense Information

Comment: Several respondents suggested that the definition of ''covered defense information'' is too expansive, requiring that data be safeguarded without clear marking instructions and identification of operational processes. Several respondents commented that contractors should not be required to make independent decisions regarding whether information is subject to safeguarding requirements, and that the rule limit its application only to covered defense information marked or expressly identified as protected by DoD. One respondent requested clarification that the rule only imposes restrictions on covered defense information that DoD provides to the contractor to perform the contract. Another respondent suggested that the relationship between ''controlled defense information'' and ''controlled unclassified information'' and the ''Controlled Unclassified Information Registry (CUI Registry)'' should be clearly articulated. Two respondents suggested that covered data be limited to the ''unclassified controlled technical information'' covered in the predecessor DFARS rule. One of the respondents further suggested that if the scope is not focused back to the ''unclassified controlled technical information'' definition, the rule should define covered defense information to specifically exclude the contractor's own information that is not delivered to the Government. One respondent commented that, because it is not possible to contemplate every type of information that may arise in the future, it would be prudent to set forth in the rule a centralized process that contractors could use when it is not clear whether a specific type of information falls within the definition of ''covered defense information'' to ensure that information is treated consistently across contracts and commands. This respondent further stated that the rule should provide a standard for evaluating whether a contractor has reasonably complied with the rule when faced with a judgment call as to whether information falls within the definition.

Response: The final rule clarifies the definition of ''covered defense information'' and the requirement to provide adequate security. The definition of ''covered defense information'' is amended to state that covered defense information is unclassified controlled technical information or other information (as described in the CUI Registry at *http://www.archives.gov/cui/registry/category-list.html*) that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies and is either (1) marked or otherwise identified in the contract and provided to the contractor by or on behalf of DoD in connection with the performance of the contract; or (2) collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract. This revised definition adds an affirmative requirement for Government to mark or otherwise identify in the contract all covered defense information that is being provided to the contractor, while recognizing the shared obligation of the contractor to recognize and protect covered defense information that the contractor is developing during contract performance. In addition, paragraph (b) of DFARS clause 252.204–7012 is amended to clarify that adequate security is required on all covered contractor information systems. Paragraph (m)(1) of the clause is also modified to indicate that, if necessary, the contractor shall determine if the information required for subcontractor performance retains its identity as covered defense information and will require protection under this clause and, if necessary, consult with the contracting officer.

b. Export Control

Comment: Several respondents suggested that the definition of covered defense information should refer only to export controlled information, and not include a general description of the type of information that may be subject to export controls. One respondent suggested this section be reworded as follows: ''Unclassified information concerning items requiring licenses under the export administration regulations, or the international trafficking in arms regulations and munitions list.'' Another respondent suggested that DoD define ''export controlled information'' in the final rule, since particular categories of International Traffic in Arms Regulations (ITAR)—controlled technical data and designated control list categories of the Export Administration Regulations (EAR), such as national security, nonproliferation, and missile technology. Several respondents suggested the definition of ''export control'' be limited to technologies subject to the EAR, ITAR, or nuclear export regulations. One respondent suggested that DoD exclude items from its definition of ''covered defense information'' that are subject to minimal export controls.

Response: The definition of ''covered defense information'' is amended to clarify that the information includes unclassified controlled technical information or other information (as described in the CUI Registry) that is marked or otherwise identified in the contract and provided to the contractor by or on behalf of DoD in connection with the performance of the contract; or be collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract. Export control is a category in the CUI Registry, but it is only considered covered defense information when both DoD contractors hold unclassified information that is export controlled, and the information is ''provided to the contractor by or on behalf of DoD in connection with the performance of the contract, or collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract,'' as defined in the final rule. Protecting DoD-related export controlled information as covered defense information should not be interpreted to imply that the same information, not related to the DoD activity, requires protection as covered defense information.

c. Covered Defense Information—''Other'' Category

Comment: Several respondents commented that DoD should provide more clarity regarding the categories of information that comprise covered defense information, specifically the scope of ''any other information. . . .'' One respondent suggested that the rule specifically address DoD information routinely handled by Contractors, such as information marked ''For Official Use Only'' and personally identifiable information (PII) maintained to support DoD clearance processing, and clearly indicate whether this information is in or out of scope. Another respondent suggested that the definition of ''covered defense information'' should be amended to exclude information, such as protected health information (PHI) that is already subject to security control regulations.

Response: The definition of ''covered defense information'' is amended to clarify that ''other information'' is other information (as described in the CUI Registry) that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies. The CUI Registry includes personal information, PII, and PHI. The security requirements in this clause set a baseline standard. Additional protections may be required for specific categories of information, such as PHI.

d. Operationally Critical Support and Critical Information (Operations Security)

Comment: Several respondents commented on how the rule addresses ''operationally critical support'' and ''critical information (operations security)'' and requested clarification of the terms ''critical information'' and ''operations security.'' One respondent commented that the rule indicates that the Government will designate which supplies or services are critical for airlift, etc., but the rule neither indicates where such information will be found, nor defines a process for designating contractors in this category or notifying such contractors that they are critical to operational support. Another respondent suggested that while the interim rule suggests that DoD will designate specific portions of its contracts that it considers to be ''operationally critical support,'' the scope of what constitutes a contractor's ''ability to provide operationally critical support'' is so vague that it may not accomplish its purpose. This respondent recommended that DoD clarify that a reportable incident occurs when a cyber incident affects the security or integrity of operationally critical information residing in a contractor information system. One respondent commented that ambiguities with regard to operationally critical support are particularly concerning to the transportation industry, suggesting that it is not clear whether ''package level detail'' which includes information about the identity of the shipping and receiving parties and the delivery address is considered ''covered defense information.'' This respondent also suggested that a cyber incident that affects the contractor's ability to perform ''operationally critical support'' could also include incidents on systems beyond ''covered information systems'' and the interim rule requires reporting of those incidents, as well. Another respondent requested DoD clarify how or whether the term ''operationally critical'' applies to contractors/subcontractors.

Response: The modified definition of covered defense information replaces the requirement that information ''falls in any of the following categories: Controlled technical information, critical information (operations security), export control, and any other information, marked or otherwise identified in the contract, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies'' with the statement ''as described in the CUI Registry at *http://www.archives.gov/cui/registry/category-list.html,* requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies.'' Because ''critical information (operations security)'' is not currently listed on the CUI Registry, it can no longer, in and of itself, be designated as covered defense information. Section 1632 of the NDAA for FY 2015, which requires that a contractor designated as operationally critical report each time a cyber incident occurs on that contractor's network or information systems, is implemented via the DFARS clause 252.204–7012 requirement for contractors and subcontractors to report cyber incidents that result in an actual or potentially adverse effect on a their ability to provide operationally critical support. Operationally critical support is an ''activity''—not an information type—performed by the contractor or subcontract. DFARS does not require protections for contractor information systems that are used to provide operationally critical support, but does require the contractor to report a cyber incident that affects the contractor's ability to perform the requirements of the contract that are designated as operationally critical support. Operationally critical support requirements must be marked or otherwise identified in the contract, task order, or delivery order.

4. Compliance

a. Multiple Versions/Block Change

Comment: Several respondents commented that the new rule could leave contractors subject to different security standards depending on which version of clause 252.204–7012 appears in their contracts and subcontracts. One respondent suggested that this results in them incurring costs due to the changes involved. Other respondents recommended that, in lieu of each contractor negotiating the phase-in relief provided in the amended rules on every transaction, DoD issue a block change modification to all contracts where the relevant August interim rule clauses are present to adopt the December 30 changes and allow for equitable adjustment to the contract price. One respondent suggested that DoD consider issuing instructions to contracting officers to substitute the most recent version of this clause for older versions, at the request of the contractor.

Response: The security requirements in NIST SP 800–171 build upon the table of controls contained in the November 2013 version of DFARS clause 252.204–7012. While there is additional effort for the difference, none of the effort to implement the original controls is lost. Due to the differences in the multiple versions of 252.204–7012, however, amending the contract requires procuring contracting officer authority and is generally bilateral, requiring contractor signature. ''Block changes'' and ''mass modifications'' are generally reserved for administrative changes, such as a payment office address change. There is nothing that precludes a contracting officer from considering a modification of the contract upon request of the contractor.

b. Cost

Comment: One respondent commented that the cost recovery model for complying with the interim rule is not well understood, suggesting that the cost to them and their supply base will be significant as they expand their capabilities to meet the new controls and absorb the administrative costs to oversee the supply base's compliance. The respondent recommended that the Office of the Under Secretary of Defense (Acquisition, Technology, and Logistics) work with industry to clarify cost recovery options.

Response: DoD does not develop ''cost recovery models'' for compliance with DFARS rules. The requirements levied by this rule should be treated the same as those levied by any other new DFARS rule and the cost related to compliance should be considered during proposal preparation. Contractors should continue to comply with their own internal accounting processes.

c. Certification and Oversight

Comment: A number of respondents commented on the lack of oversight and certification of compliance with the NIST controls in the rule. Several respondents requested clarification on the requirements for an organization to be considered compliant, as well as the intended means of verification, which organization will verify, how compliance will be assessed, and how

often. One respondent requested details on the process for obtaining official, consistent interpretations of the standards when DoD and the contractor have different interpretations of the NIST SP 800–171 standards. Another respondent recommended that large companies be allowed to certify at the company level, suggesting that the requirement to certify each program individually creates an insurmountable burden for both the company and DoD.

Response: No new oversight paradigm is created through this rule. If oversight related to these requirements is deemed necessary, then it can be accomplished through existing Federal Acquisition Regulation (FAR) and DFARS allowances, or an additional requirement can be added to the terms of the contract. The rule does not require ''certification'' of any kind. By signing the contract, the contractor agrees to comply with the contract's terms.

d. Implementation Deadline

Comment: One respondent asked for clarification with regard to what the term ''as soon as practical'' means.

Response: The phrase ''as soon as practical'' is added to encourage contractors to begin implementing the security requirements in NIST SP 800–171 prior to the December 31, 2017, deadline, but allows contractors to exercise their own judgement when planning an optimal implementation strategy.

e. Source Selection

Comment: One respondent inquired if DoD can require immediate compliance with all NIST controls as a condition of responsiveness to a solicitation, and urged DoD to prohibit source selection exclusions based on a desire or demand for 100% compliance at time of solicitation or contract prior to December 31, 2017. Another respondent suggested that the final rule clarify that DoD does not intend for DFARS clause 252.204–7012 to be used in the evaluation process.

Response: DFARS Clause 252.204–7012 is not structured to facilitate the use of the contractor's compliance with NIST SP 800–171 as a factor in the evaluation/source selection process. The requirements are set as the minimum acceptable level to protect covered defense information. The rule does not preclude a requiring activity from specifically stating in the solicitation that compliance with the NIST SP 800–171 will be used as an evaluation factor in the source section process, and the specifics on how such an evaluation factor would be utilized to evaluate proposals would need to be detailed within the solicitation. However, this is outside of the scope of this rule and would need to be appropriately addressed on an individual solicitation basis.

5. 30-Day Notification and Alternative Controls

a. Notification Versus Alternatives

Comment: Several respondents requested clarification as to why DFARS 252.204–7008 and 252.204–7012 are separate. Other respondents suggested that there is a contradiction between DFARS provision 252.204–7008 and clause 252.204–7012, and requested clarification regarding the intent of the 30-day notification requirement. Respondents also requested that DoD clarify how the NIST controls requirements variance process identified in the representation clause at 252.204–7008 (*i.e.,* a written explanation and adjudicative process by the DoD CIO pre-award) differs from the security clause at 252.204–7012, which allows for phased-in implementation with a process of proposing alternatives without pre-award approval.

Response: DFARS provision 252.204–7008 serves as a notice to offerors. The provision puts the offeror on notice that, when performance of the contract requires covered defense information on a covered contractor information system, the security requirements in NIST SP 800–171 apply and must be implemented no later than December 31, 2017. In addition, the provision notifies the offeror that they may submit a request to vary from any of the security requirements in NIST SP 800–171 to the contracting officer, for adjudication by DoD CIO, prior to award. DFARS clause 252.204–7012 is amended by adding a new paragraph (b)(2)(ii)(B) to clarify that the contractor may submit a request to vary from the security requirements in NIST SP 800–171 after contract award.

Separate and distinct from the process to request to vary from the security requirements in NIST SP 800–171, the 30-day notification requirement contained in DFARS clause 252.204–7012 requires the contractor to provide the DoD CIO with a list of the security requirements that the contractor is not implementing at the time of award. This notification will end for all contracts awarded after September 30, 2017, in preparation of the full security requirement implementation date of December 31, 2017.

b. Alternative Controls

Comment: Several respondents requested that DoD clarify 252.204–7008 with regard to the process to request variances from the SP 800–171 security controls, to include where a contractor/subcontractor request should be sent, if subcontractors may bypass their prime contractor when submitting in order to safeguard any proprietary information, a timeline for the authorized representative from the DoD CIO's office to respond to contractor/subcontractor requests, and whether and how CIO evaluations could impact award decisions. One respondent recommends that DoD clarify that contractors may also identify and seek CIO adjudication on variances from NIST SP 800–171 requirements after award as they progress through implementation, and that DoD clarify that such documents will be securely maintained and not be released publicly.

Response: DFARS provision 252.204–7008 ensures that offerors are aware of the safeguarding requirements of DFARS clause 252.204–7012, and provides a process for the offeror to identify situations in which a security requirement in NIST SP 800–171 is not necessary in performance of the contract, or to propose an alternative to a security requirement is NIST SP 800–171. In such cases, the offeror must provide a written explanation in their proposal describing the reasons why a security requirement is not applicable, or how alternative, but equally effective, security measures can compensate for the inability to satisfy a particular requirement. The contracting officer will refer the proposed variance to the DoD CIO for adjudication. The DoD CIO is responsible for ensuring consistent adjudication of proposed non-applicable or alternative security measures. If the DoD CIO needs additional information, a request is made to the contracting officer. Responses are then returned to the contracting officer who, in turn, advises the contractor of the decision. The timeframe for response by the DoD CIO is typically within five business days. The basis for determining if an alternative to a security requirement is acceptable is whether the alternative is equally effective; the basis for determining a security requirement is ''not applicable'' is whether the basis or condition for the requirement is absent. While the scope of this rule does not provide for the CIO evaluation to impact the award decision, there is nothing that precludes an activity from drafting the solicitation to provide for this.

DFARS clause 252.204–7012 is amended by adding a new paragraph

(b)(2)(ii)(B) to clarify that the contractor may request the contracting officer seek DoD CIO adjudication on variances from NIST SP 800–171 requirements after award. DFARS clause 252.204–7012 is flowed down to subcontractors without alteration when performance will involve operationally critical support or covered defense information. However, paragraph (m) of the clause is amended to clarify that the prime contractor shall require subcontractors to notify the prime contractor (or next higher-tier subcontractor) of any requests for variance submitted directly to the contracting officer.

c. 30-Day Notification

Comment: Several respondents requested that clarification be provided regarding the requirement that the contractor provide notification to the DoD CIO within 30 days of contract award listing the unmet NIST SP 800–171 security requirements. Respondents asked the following questions: Is the 30-day deadline for the prime contractor's response only, or also for the prime's entire supply base? Would post-award notifications also be required 30 days after award of subcontracts? Should subcontractors submit their notifications directly to the DoD CIO? Can subcontractors also be required to submit copies to the prime contractor? How will these sensitive documents be protected? One respondent asked what is required for the 30-day assessment, if the contract in question ends prior to the December 31, 2017, compliance date. One respondent also suggested that the requirement should be modified to allow at least 90 days after award, and that DoD should allow for a single corporate-wide compliance, and that such a compliance requirement could be accomplished at annual or semi-annual intervals, and not on every single transaction within 30 days.

Response: DFARS clause 252.204–7012 requires the contractor to notify the DoD CIO, within 30 days of contract award, of the security requirements that are not implemented at the time of award. The list need only identify the security requirement(s) (*e.g.,* NIST SP 800–171 security requirement 3.1.1) that is/are not implemented. No additional information is required.

DFARS clause 252.204–7012 is flowed down to subcontractors without alteration when performance will involve operationally critical support or covered defense information. As such, prior to October 1, 2017, the requirement is for the subcontractor to provide the DoD CIO, within 30 days of the prime contractor's award to the subcontractor, with a list of the security requirements that the subcontractor has not implemented at the time of award. Bypassing the prime is a matter to be addressed between the prime and the subcontractor.

Nothing precludes the contractor from providing a corporate-wide update to the status of requirements not implemented on a periodic basis, assuming it meets the requirements of the clause. If the contract in question ends prior to December 31, 2017, the Contractor must still provide the DoD CIO, within 30 days of contract award, with a list of the security requirements that are not implemented at the time of award.

Comment: One respondent asked that DoD confirm/clarify that after the 30-day notification, contractors are expected to manage compliance with DFARS clause 252.204–7012 through system security plans and plans of action and milestones. The respondent also asked for clarification that the only required reporting to DoD CIO subsequent to the initial list is to identify any NIST SP 800–171 controls that a contractor does not intend to meet either because the contractor has deemed the controls to be not applicable or because mitigating controls have been implemented.

Response: The notification to the DoD CIO of the NIST–SP security requirements not implemented at the time of contract award is a one-time action per contract and is a requirement for contracts awarded prior to October 1, 2017 (see 252.204–7012(b)(2)(ii)(A)). Separately, a contractor may submit requests to vary from a NIST SP 800–171 security requirement (because it is believed to be not applicable or the contractor has an alternative in place) to the contracting officer for adjudication by the DoD CIO (see 252.204–7012(b)(2)(ii)(B)).

During the course of performance under the contract, the contractor may manage compliance with the NIST SP 800–171 security requirements through a system security plan. One of the assumptions of NIST SP 800–171 (per table E–12 of the document) is that nonfederal organizations routinely have a system security plan in place to manage and maintain their information systems. When a corrective action is necessary to maintain NIST compliance, a plan of action may be necessary in accordance with NIST 800–171 requirement 3.12. DFARS clause 252.204–7012 is updated at paragraph (b)(3) to clarify that temporary deficiencies with compliance may be addressed within a system security plan.

6. Incident Reporting and Damage Assessment

a. Reporting (When, Where, What Versus 72 Hours)

Comment: Two respondents commented on the 72-hour reporting requirement. One suggested that the 72-hour reporting requirement is unrealistic unless the rule is revised to limit its applicability to specific information that DoD has provided to the contractor or subcontractor with appropriate markings. One respondent suggested that 72 hours is not enough time to investigate a potential cyber incident, confirm the incident, and obtain the requisite report information. Several respondents commented that the increased reporting requirement to include potentially adverse effects on an information system regardless of an actual compromise to covered defense information, is too burdensome to industry for little apparent benefit, and suggested that DoD eliminate the words ''or potentially'' from the definition of cyber incident. One respondent suggested that the rule address what factors contractors should consider when evaluating whether an incident has a ''potentially adverse effect.'' One respondent recommended that a threshold be established on when a contractor and subcontractor would be required to report a cyber incident, and that the agency point of contact be a centralized figure/office in which all cyber incident reports are submitted to or, in the alternative, a centralized figure/office that handles reporting for all contracts under which a given contractor performs.

Response: When a cyber incident is discovered, the contractor/subcontractor should report whatever information is available to the DIBNet portal within 72 hours of discovery. If the contractor/subcontractor does not have all the information required on the Incident Collection Form (ICF) at the time of the report, and if more information becomes available, the contractor should submit a follow-on report with the added information. The DoD Cyber Crime Center (DC3) serves as the DoD operational focal point for receiving cyber threat and incident reporting from those Defense contractors who have a contractual requirement to report under DFARS clause 252.204–7012. Upon receipt of the contractor/subcontractor-submitted ICF in the DIBNet portal, DC3 will provide the submitted ICF to the contracting officer identified on the ICF. The contracting officer is directed in DFARS Procedures, Guidance, and Information 204.7303–3 to notify the

requiring activities that have contracts identified in the ICF.

b. Incident Collection Form

Comment: One respondent recommended that the ICF, for example on the DIBnet site, should include a field where the contractor can indicate the vulnerability suspected, known, or created.

Response: The ICF fields are described at the ''Resources'' tab at *http://dibnet.dod.mil.* Field numbers 16 (Type of compromise), 17 (Description of technique or method used in cyber incident), 19 (Incident/Compromise narrative), and 20 (Any additional information) each provide the opportunity for the contractor to indicate the vulnerability suspected.

d. Access to Contractor Information

Comment: Multiple respondents commented that the rule does not appropriately limit the Government's access to contractor systems and fails to adequately protect sensitive contractor data, suggesting that the rule be revised to recognize the need for appropriate limits on the Government's rights to request, use, and disclose sensitive contractor information it may obtain as a result of a reported cyber incident or investigation. Many respondents offered alternatives of how to limit access. Several respondents suggested that the final rule use the same use and disclosure rights that were contained in the prior unclassified controlled technical information (UCTI) rule. Others suggested that the rule be modified to state that DoD limit access to equipment or information only in connection with a contractor report of a ''cyber incident'' and as necessary to conduct a forensic analysis or damage assessment, adding that the parties should discuss in good faith whether additional information or equipment is necessary. One suggested that the rule indicate that the Government may require access to equipment or information only ''to determine whether information created by or for the Department in connection with any Department program was successfully exfiltrated from a network or information system and, if so, what information was exfiltrated.''

Response: This rule adds on to the prior UCTI rule, by implementing 10 U.S.C. 391 and 393 (previously section 941 of the NDAA for FY 2013 and section 1632 of the NDAA for FY 2015), which state that contractors will provide access to equipment or information to determine if DoD information was successfully exfiltrated from a network or information system of such contractor and, if so, what information was exfiltrated. This requirement is implemented in DFARS clause 252.204–7012 by stating that, upon request by DoD, the Contractor shall provide DoD with access to additional information or equipment that is necessary to conduct a forensic analysis—thus limiting DoD access to equipment/information necessary to conduct the analysis resulting from a cyber incident, as suggested above. This analysis is critical to understand what information was exfiltrated from the information system.

e. Protection/Use of Contractor Information

Comment: Multiple respondents commented that the interim rule should address how DoD will safeguard any contractor data provided. One respondent added that the clause also does not allow contractors an opportunity to review their security information before it is disclosed. Several respondents recommend that the final rule use the same use and disclosure rights that were contained in the prior UCTI rule. One respondent recommended that DoD make clear that the information it receives from contractors under the cyber incident reporting rules may not be used for Government commercial or law enforcement purposes. One respondent suggested that the rule should address personal information in internal contractor systems, recommending that the DoD Privacy Officer review the rule and conduct a privacy impact assessment, and that DoD address special procedures and protections for personal information. One respondent suggested that the DFARS prohibit the release outside DoD of PHI or PII provided to DoD in connection with the reporting or investigation of a cyber incident.

Response: DoD protects against unauthorized use or release of cyber incident reporting information from the contractor, in accordance with applicable statutes and regulations. DoD complies with 10 U.S.C. 391 and 393 and provides reasonable protection of trade secrets and other information, such as commercial or financial information, and information that can be used to identify a specific person. DoD limits the dissemination of cyber incident information to the entities specified in the rule.

f. Attributional/Proprietary Information

Comment: One respondent suggested that the definition of contractor attributional/proprietary information exceeds the stated scope of the subpart 204.7300, namely, ''to safeguard covered defense information that resides in or transits through covered contractor information systems.'' One respondent commented that the rule places the burden on the contractor to mark information as ''contractor attributional/proprietary,'' adding that the rule should either address how contractors can protect previously unmarked information while still complying with the requirement to preserve images of their information system, or enumerate what steps the Government will take to ensure that the absence of a marking on a document provided to the Government as part of that image will not be treated as determinative of the Government's ultimate obligations to protect that information as contractor attributional/proprietary.

One respondent commented that restrictions and requirements imposed by the rule with regard to attributional/proprietary information would impact international suppliers of U.S. allies who provide critical components that are integrated into major systems and subsystems, suggesting that international suppliers may be unable to comply with the requirements of the DFARS due to the applicable laws in their country or a lack of resources.

Response: The Government may request access to media to assess what covered defense information was affected by the cyber incident. DoD will protect against the unauthorized use or release of contractor attributional/proprietary information. The contractor should identify and mark attributional/proprietary information and personal information to assist DoD in protecting this information. To the extent that media may include attributional/proprietary information, the Government will protect against unauthorized access. DoD will need to work with the prime contractor to resolve challenges with international suppliers on a case by case basis.

g. Third Party Information

Comment: Several respondents commented on third-party support contractors' access to other contractors' internal systems and/or information. One respondent suggested that third party support contractor access to other contractors' internal systems raises serious concerns and encouraged DoD to incorporate an effective mechanism to notify the originating party about third parties with access to such data, as well as any disclosure of such data by those third parties. One respondent recommended that DoD add a requirement for third parties to sign a non-disclosure agreement with each

company they may conduct a forensic analysis on or an investigation against.

Response: The rule subjects support service contractors directly supporting Government activities related to safeguarding covered defense information and cyber incident reporting (*e.g.,* providing forensic analysis services, damages assessment services, or other services that require access to data from another contractor) to restrictions on use and disclosure obligations.

h. Liability Protections

Comment: One respondent recommended that the final rule integrate the liability protections provided by section 1641 of the NDAA for FY 2016, further suggesting that DoD work to extend the liability protections so that all contractors and subcontractors that are required to report cyber incidents under its regulations are provided the same levels of protection.

Response: DFARS Case 2016–D025, Liability Protections when Reporting Cyber Incidents, was opened on April 20, 2016 to implement section 1641 of the FY 2016 NDAA.

7. Subcontractors

a. Reporting

Comment: Multiple respondents addressed the requirement for subcontractors to simultaneously report incidents directly to the Government and the prime contractor. One respondent suggested that having subcontractors report directly to DoD creates a control challenge for prime contractors. Another suggested that subcontractor reporting directly to DoD removes the prime contractors ability to educate themselves about the incident and to be a resource to DoD. Others suggested that the obligation for subcontractors to report violates the subcontractor's confidentiality rights. Other respondents requested clarification regarding the types of information that must be disclosed by subcontractors to prime contractors. One respondent suggest the rule should limit the information that a subcontractor is required to report to its prime contractor or, otherwise, limit the prime contractors' ability to disclose any information that is received as a result of the disclosures. One respondent commented that it is not clear how the Government intends to protect proprietary information reported by the subcontractor to the prime contractor from unauthorized use.

Response: The rule has been amended to clarify that subcontractors are required to rapidly report cyber incidents directly to DoD at *http://dibnet.dod.mil,* and to provide the incident report number, automatically assigned by DoD, to the prime Contractor (or next higher-tier subcontractor) as soon as practicable. Any requirement for the subcontractor to provide anything more than the incident report number to the prime Contractor (or next higher-tier subcontractor) is a matter to be addressed between the prime and the subcontractor.

DoD will protect against the unauthorized use or release of cyber incident information reported by the contractor or subcontractor in accordance with applicable statutes and regulations.

b. Flowdown

Comment: Multiple respondents commented on aspects of the flowdown and subcontractor requirements of the rule. One respondent asked which party determines whether a subcontractor's efforts involve covered defense information or require providing operationally critical support, suggesting that, without additional detail or guidance, the determination of what constitutes covered defense information or operationally critical support would vary. Several respondents requested clarification regarding how DoD intends to enforce the flowdown of DFARS clause 252.204–7012 beyond the first tier of the supply chain, and how subcontractors can comply with the final rule's requirements. One respondent asked DoD to clarify whether it will prohibit a prime contractor from entering into a subcontract if the subcontractor refuses to accept DFARS 252.207–7012. Several respondents commented on the change made to the second interim rule that, when applicable, the clause shall be included without alteration, except to identify the parties, suggesting that this requirement restrains prime contractors' and subcontractors' ability to negotiate flowdown provisions that address the specific needs of their contractual arrangements. Another asked if ''where DoD requires flow-down without alteration, can industry assume that wherever the language in 252.204–7012 refers to a ''contractor,'' the term ''subcontractor'' should or can be used in the flowdown version of the clause, except where ''subcontractor'' is already used in the clause''?

Response: Paragraph (m) of DFARS clause 252.204–7012, states that the clause will be included without alteration, ''except to identify the parties.'' This allows the Contractor to identify the appropriate party as required. Paragraph (m) is amended in the final rule to clarify that flowdown of the clause is required for subcontracts for operationally critical support, or for which subcontract performance will involve ''covered defense information,'' instead of ''a covered contractor information system.'' Paragraph (m) is further amended to instruct the contractor to, if necessary, consult with the contracting officer to determine if the information required for subcontractor performance retains its identity as covered defense information and will require protection under this clause, thus driving when the substance of DFARS clause 252.204–7012 must be included in a subcontract. Flowdown is a requirement of the terms of the contract with the Government, which should be enforced by the prime contractor as a result of compliance with these terms. If a subcontractor does not agree to comply with the terms of 252.204–7012, then covered defense information shall not be on that subcontractor's information system.

8. Cloud Computing

a. Access

Comment: One respondent commented that they did not agree with DFARS 252.239–7010(i)(3), ''which provides that a Government contracting officer may require physical access to data centers for purposes of audits, inspections, or other similar and undefined activities,'' suggesting that the DFARS be revised to reflect the practice of infrastructure as-a-service providers to limit third party access to data centers to accredited FedRAMP third party assessment organizations and to law enforcement activities.

Response: DFARS 252.239–7010(i)(3) states that the contractor shall provide the Government or its authorized representatives (vice contracting officers) access to all Government data and Government-related data, access to contractor personnel involved in performance of the contract, and physical access to any Contractor facility with Government data, for the purpose of audits, investigations, inspections, or other similar activities, as authorized by law or regulation (vice undefined activities).

b. 252.204–7012 Versus 252.239–7010

Comment: One respondent commented that it is unlikely that a majority of CSPs have completed their review/audit of their systems in order to notify contracting officers within 30 days of award whether or not they comply with NIST SP 800–171 security

requirements. This respondent also commented that companies that have demonstrated compliance with DoD Impact Level L4/5 (as described in the Cloud Computing Security Requirements Guide (SRG)) should not be required to do all the paperwork or be subject to the requirement for an additional assessment.

Response: When using cloud computing to provide information technology services in the performance of the contract (*i.e.,* an information technology service or system operated on behalf of the Government), CSPs shall comply with the requirements of DFARS Clause 252.239–7010, Cloud Computing Services, which points to the Cloud Computing SRG. The requirement to provide DoD CIO with a list of security requirements that are not implemented at the time of contract award applies only to implementation of security requirements as required in DFARS clause 252.204–7012. The rule has been amended to clarify that when the contractor is not providing cloud computing services in the performance of the contract, but intends to use an external CSP to store, process, or transmit any covered defense information for the contract, DFARS clause 252.204–7012 (b)(2)(ii)(D) applies. DFARS clause 252.204–7012(b)(2)(ii)(D) requires the CSP to meet security requirements equivalent to those established by the Government for the FedRAMP ''Moderate'' baseline at the time award. The text in DFARS clause 252.204–7012 has also been amended to clarify that the contractor shall, within 30 days of contract award, provide the DoD CIO with a list of the security requirements at (b)(2)(i) that are not implemented at the time of contract award, to include any security requirements not implemented by an external cloud service provider.

Comment: One respondent suggested that the rule does not provide any guidance as to how to reconcile the implementation of DFARS clauses 252.204–7012 and 252.239–7010, and that the appropriate security controls that should be applied to cloud systems is unclear. The respondent suggested that because the cloud computing exemption in DFARS 252.204–7012 is located within the ''adequate security'' requirements of the clause, the clause can be read as to impose the Cloud Computing SRG security requirements (included in 252.239–7010) on all cloud information systems, and that different reporting and preservation requirements would apply if the information stored on the CSP's cloud is covered defense information. This respondent further suggested that the scope of DFARS 252.204–7012(b)(1)(A) is defined by the type of service provided, rather than the environment in which information is stored.

Response: DFARS clause 252.204–7012 has been amended to clarify the appropriate security controls that should be applied on all covered contractor information systems. Cyber incident reporting, media preservation, and system access are not part of the contractor's adequate security obligations, but rather distinct requirements of the clause when a cyber incident occurs on a covered contractor information system.

Comment: One respondent commented that it is unclear whether the exemption for security controls contained within DFARS 252.204–7012 covers ancillary cloud services, such as cloud migration and eDiscovery, that a CSP may provide as an add-on service to a cloud computing contract. This respondent suggested that a clarification of the scope of the exemption would be helpful for defining reporting and safeguarding obligations for these providers. One respondent suggested that DoD revise DFARS clause 252.204–7012 to clarify that data stored on a cloud is exempt from the requirements of this clause and subject only to the requirements of DFARS clause 252.239–7010. Such an approach will provide contractors with clear guidelines as to when they are subject to the requirements DFARS 252.204–7012 or DFARS 252.239–7010. Furthermore, through the application of the Cloud Computing SRG requirements to data stored on a cloud, this approach will ensure that DoD information receives the appropriate degree of protection for the environment in which it is stored.

Response: DFARS clause 252.204–7012 requires that (for an information technology service or system operated on behalf of the Government) CSP shall comply with the requirements of DFARS clause 252.239–7010, Cloud Computing Services, which points to the Cloud Computing SRG (see paragraph (b)(1)(i) of the clause). This clause has been amended to clarify that (for an information technology services or system not operated on behalf of the Government) when using an external CSP to store, process, or transmit any covered defense information, the CSP shall meet requirements equivalent to those established by the Government in the FedRAMP Moderate baseline (see paragraph (b)(2)(ii)(D) of the clause).

Comment: One respondent commented that they understand that the subcontractor flowdown clause is not required in contracts between the contractor and the CSPs, and that the contractor is not responsible for ensuring that CSPs comply with DFARS clause 252.204–7012, and requested that this be confirmed or clarified.

Response: When a contractor uses an external CSP to store, process, or transmit any covered defense information for the contract, DFARS Clause 252.204–7012(b)(2)(ii)(D) applies. While the flowdown provision in 252.204–7012 does not apply to the CSP in this case, the prime contractor is responsible to ensure that the CSP meets the requirements at 252.204–7012(b)(2)(ii)(D).

c. Reporting

Comment: One respondent commented that the rule fails to define the information that must be reported and creates a reporting system separate from the FedRAMP and Cloud Computing SRG Requirements, suggesting that an established system with clear reporting requirements for cloud computing security incidents would be more efficient than utilizing a new, separate, possibly conflicting portal at *http://dibnet.dod.mil.*

Response: The public facing DIBNet Web site includes a ''Resources'' tab that describes the information required when reporting a cyber incident that is related to the cloud computing service provided under his contract. Consistent with reporting requirements in DFARS clause 252.205–7012 and the Cloud Computing SRG, reports shall be submitted to DoD via *http://dibnet.dod.mil/.* This is DoD's single reporting mechanism for DoD contractor reporting of cyber incidents on unclassified information systems. The rule streamlines the reporting processes for DoD contractors and minimizes duplicative reporting processes.

Comment: One respondent commented that it is their understanding that if a contractor, when not providing information technology services in the performance of the contract, but is using an external CSP that is FedRAMP compliant to store, process, or transmit any covered defense information for the contract, the contractor only needs to ensure that the CSP reports cyber incidents to the contractor so the contractor can comply with its reporting requirements to the Government.

Response: DFARS clause 252.204–7012 was amended to require that the CSP should be FedRAMP ''Moderate'' compliant, not simply FedRAMP compliant (as there are CSPs that are only FedRAMP ''Low'' compliant, which is not sufficient for covered defense information protection). The clause also requires that the external

CSP meets the cyber incident reporting, malicious software, media preservation and protection, access to additional information and equipment necessary for forensic analysis, and cyber incident damage assessment requirements at paragraphs (c) through (g) of the clause.

Comment: One respondent suggested that CSPs should only be responsible for reporting incidents that result in an actual, or reasonably suspected, unauthorized disclosure of customer data, adding that if reporting requirements are scoped to customer data only, then the 72-hour reporting window is reasonable.

Response: Cyber incidents that impact the environment could have an impact on the CSP's security accreditation and DoD data, which is the reason that all incidents that are on shared services and infrastructure should be reported.

Comment: One respondent commented that the reporting requirements in DFARS clause 252.239–7010 fail to recognize the unique role of CSPs, stating that commercial CSPs and their customers typically agree to abide by strict privacy and access-to information controls which normally include limiting provisions that prevent CSPs from accessing customer information without prior consent and from providing customer data to third parties or providing third parties access to customer data. The respondent suggested that these limitations, in which only the customer would know whether an incident impacts a particular customer's data and whether there are additional reporting requirements, drive the need for a two-step reporting requirement that allows the customer who has full knowledge of the data that is stored in the cloud and the applicable classifications of such data to make the ultimate determination of any reporting obligations to the Government.

Response: As any cyber incident to the shared infrastructure can have an adverse impact on DoD data, the CSP must report any cyber incident to the shared infrastructure to DoD. That may require modifications to their commercial terms of service to allow for that. In addition, communication between the Government and the contractor (whether CSP or not) is vital; any specific requirements, or interpretations of requirements, should be negotiated as part of the service level agreement.

Comment: Several comments suggested that DFARS 252.239–7010, Cloud Computing Services, sets forth a number of requirements that commercial cloud infrastructure (*i.e.,* infrastructure as a service (IaaS)) providers will not be able to sign up to (as prime contractors or subcontractors), because compliance with those requirements are outside of their control; compliance with those requirements falls within the control of the managed services providers, account owners, lead systems engineers, or prime contractors (the ''primes'') running DoD workloads and storing ''Government data'' and ''Government-related data'' in the cloud infrastructure. One comment suggested that the DIBNet cyber reporting requirements should not apply to IaaS providers, but to the prime using the cloud, stating that although IaaS providers will notify the primes of security breaches, they will not have insight into the nature of the data the primes are storing and processing in the infrastructure, or know whether a breach results in a ''cyber incident,'' as that term is defined in the clause.

Response: The reporting requirement in DFARS 252.239–7010 requires the prime to report all cyber incidents that are related to the cloud computing service provided under the contract. In cases where the CSP is the prime contractor, the provider is required to report the incident to DoD. If the provider (acting as a prime) does not have insight into the nature of the data being stored or processed, any breach would be considered a cyber incident given the potential impact it could have on the information or the information system.

Because the IaaS providers deliver shared services, any cyber incident on the shared infrastructure and services would be the responsibility of the IaaS provider and they are obligated to report those incidents.

9. Workforce Training

Comment: One respondent asked about DoD plans to train the workforce to consistently apply the requirements for handling covered defense information.

Response: DoD will engage across both Government and industry to educate and raise awareness of the importance of protecting covered defense information. The Better Buying Power 3.0 initiative includes efforts to educate our workforce on the value and best practices for system security and efforts to communicate the importance of cybersecurity across DoD and to the Defense Industrial Base. Efforts to improve technological superiority will be in vain if effective cybersecurity is not practiced throughout the product lifecycle. Defense Acquisition University, in coordination with education counterparts in the Intelligence Community and Defense Security Service, is working to develop education and training to increase workforce understanding of the value and best practices for covered defense information protection.

C. Other Changes

The following additional changes are made in the final rule:

1. Definitions. Several definitions already included in the rule are added to or removed from certain subparts based on their usage in the text, to include ''compromise,'' ''information system,'' ''media,'' ''operationally critical support,'' ''spillage,'' and ''technical information.''

2. Incident Report Number. DFARS 204.7302(b) and 252.204–7012(m)(2)(ii) are amended to clarify that the incident report number is automatically assigned by DoD.

3. NIST SP 800–171. DFARS 252.204–7008(c) is amended to clarify in the notice to offerors, the requirement to implement the NIST SP 800–171 that is in effect at the time the solicitation is issued or as authorized by the contracting officer.

4. Malicious Software. DFARS 252.204–7012(d) is amended to specifically direct the contractor to not send malicious software to the contracting officer.

5. Access. DFARS 239.7602–1 is amended to provide the same list provided at DFARS 252.239–7010(i)(3) of activities in which the contractor is required to provide records and facility access.

D. Additional Information

Defense Procurement and Acquisition Policy (DPAP) Program Development and Implementation (PDI) provides answers to frequently asked questions at *http://www.acq.osd.mil/dpap/pdi/network_penetration_reporting_and_contracting.html.* The answers to these general questions are intended to assist with understanding and implementing the requirements of this rule.

III. Applicability to Contracts at or Below the Simplified Acquisition Threshold and for Commercial Items, Including Commercially Available Off-the-Shelf Items

The rule created two new provisions and two new clauses as follows: (1) DFARS 252.204–7008, Compliance with Safeguarding Covered Defense Information Controls; (2) DFARS 252.204–7009, Limitations on the Use or Disclosure of Third-Party Contractor Information; (3) DFARS 252.239–7009, Representation of Use of Cloud Computing; and (4) DFARS 252.239–7010, Cloud Computing Services.

Additionally, the rule amended the existing DFARS clause 252.204–7012, Safeguarding Covered Defense Information and Cyber Incident Reporting.

The objectives of the rule are to improve information security for DoD information stored on or transiting contractor information systems as well as in a cloud environment. The rule implements section 941 of the NDAA for FY 2013 (Pub. L. 112–239), section 1632 of the NDAA for FY 2015, and section 325 of the Intelligence Authorization Act of FY 2014 (Pub. L. 113–126). Additionally the rule implements DoD CIO policy for the acquisition of cloud computing services. The only clause within this rule that is implementing the statutory requirements is clause 252.204–7012, which already applied to acquisitions below the simplified acquisition threshold (SAT) and to commercial items, including commercially available off-the-shelf items (COTS). The following addresses the applicability of the new statutory requirements in DFARS clause 252.204–7012.

A. Applicability to Contracts at or Below the SAT

41 U.S.C. 1905 governs the applicability of laws to contracts or subcontracts in amounts not greater than the simplified acquisition threshold (SAT). It is intended to limit the applicability of laws to such contracts or subcontracts. 41 U.S.C. 1905 provides that if a provision of law contains criminal or civil penalties, or if the FAR Council makes a written determination that it is not in the best interest of the Federal Government to exempt contracts or subcontracts at or below the SAT, the law will apply to them. The Director, DPAP, is the appropriate authority to make comparable determinations for regulations to be published in the DFARS, which is part of the FAR system of regulations.

B. Applicability to Contracts for the Acquisition of Commercial Items, Including COTS Items

41 U.S.C. 1906 governs the applicability of laws to contracts for the acquisition of commercial items, and is intended to limit the applicability of laws to contracts for the acquisition of commercial items. 41 U.S.C. 1906 provides that if a provision of law contains criminal or civil penalties, or if the FAR Council makes a written determination that it is not in the best interest of the Federal Government to exempt commercial item contracts, the provision of law will apply to contracts for the acquisition of commercial items. Likewise, 41 U.S.C. 1907 governs the applicability of laws to commercially available off-the-shelf (COTS) items, with the Administrator for Federal Procurement Policy the decision authority to determine that it is in the best interest of the Government to apply a provision of law to acquisitions of COTS items in the FAR. The Director, DPAP, is the appropriate authority to make comparable determinations for regulations to be published in the DFARS, which is part of the FAR system of regulations.

C. Applicability Determination

The Director, DPAP, has determined that it is in the best interest of the Government to apply the requirements of section 941 of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2013, section 1632 of the NDAA for FY 2015, and section 325 of the Intelligence Authorization Act of FY 2014 (Pub. L. 113–126) to contracts at or below the SAT and to contracts for the acquisition of commercial items, for clause 252.204–7012, Safeguarding Covered Defense Information and Cyber Incident Reporting. However, the clause prescription is amended in the final rule to exempt use in solicitations and contracts that are solely for the acquisition of COTS items.

The necessity to protect covered defense information is the same across all contract types for all dollar values. The harm that could result from the loss or compromise of covered defense information is the same under a FAR part 12 contract that is under the SAT as it would be under any other contract. Recent high-profile breaches of Federal information show the need to ensure that information security protections are clearly, effectively, and consistently addressed in contracts. Failure to apply this rule to contracts with covered defense information may cause harm to the Government which could directly impact national security. Therefore, exempting contracts below the SAT or for the acquisition of commercial items (excluding COTS items) from application of the statutes would severely decrease the intended effect of the statutes and increase the risk of mission failure.

For the same reasons expressed in the preceding paragraph, DoD applied the following provisions and clauses to acquisitions below the SAT and to the acquisition of commercial items, excluding COTS items: (1) DFARS 252.204–7008, Compliance with Safeguarding Covered Defense Information Controls; (2) DFARS 252.204–7009, Limitations on the Use or Disclosure of Third-Party Contractor Information; (3) DFARS 252.239–7009, Representation of Use of Cloud Computing; and (4) DFARS 252.239–7010, Cloud Computing Services.

IV. Executive Orders 12866 and 13563

Executive Orders (E.O.s) 12866 and 13563 direct agencies to assess all costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributive impacts, and equity). E.O. 13563 emphasizes the importance of quantifying both costs and benefits, of reducing costs, of harmonizing rules, and of promoting flexibility. This is not a significant regulatory action and, therefore, was not subject to review under section 6(b) of E.O. 12866, Regulatory Planning and Review, dated September 30, 1993. This rule is not a major rule under 5 U.S.C. 804.

V. Regulatory Flexibility Act

A final regulatory flexibility analysis (FRFA) has been prepared consistent with the Regulatory Flexibility Act, 5 U.S.C. 601, *et seq.* The FRFA is summarized as follows:

This final rule expands on the existing information safeguarding policies in the Defense Federal Acquisition Regulation System (DFARS), which were put in place in November 2013 (78 FR 69273), by requiring contractors to report cyber incidents to the Government in a broader scope of circumstances.

The objective of this rule is to implement section 941 of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2013 (Pub. L. 112–239), section 1632 of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2015, and DoD CIO policy for the acquisition of cloud computing services, in order to improve information security for DoD information stored on or transiting contractor information systems, as well as in a cloud environment.

The significant issues raised by the public in response to the initial regulatory flexibility analysis are as follows:

Comment: Respondents expressed concern that the estimated of the total number of small businesses impacted by the rule is too low and that the rule does not allow for alternative standards or exemption for small business due to potentially burdensome costs of compliance.

Response: As there is no database collecting the number of contractors receiving covered defense information it is difficult to determine how many contractors are required to implement the security requirements of clause 252.204–7012, Safeguarding Covered Defense Information and Cyber Incident Reporting. Further, without adding a new information collection requirement to prime contractors it is not possible to determine how many subcontractors are in possession of covered defense information. Based on the respondent's analysis of the number of small entities, as prime contractors and as subcontractors, that may be affected by the rule the DoD estimate of small entities affected by this rule has been revised, to increase the number.

The cost of compliance with the requirements of this rule is unknown as the cost is determined based on the make-up of the information system and the current state of security already in place. If a contractor is already in compliance with the 2013 version of the clause 252.204–7012, then the changes necessary to comply with the new rule are not as significant. For a new contractor that has not been subject to the previous iteration of the 252.204–7012 clause and is now handling covered defense information the cost could be significant to comply. The cost of compliance is allowable and should be accounted for in proposal pricing (in accordance with the entity's accounting practices). Though it is not a change specific to small entities the security requirements as amended in this rule are found in National Institute of Standards and Technology (NIST) Special Publication (SP) 800–171, ''Protecting Controlled Unclassified information in Nonfederal Information Systems and organizations,'' to replace a table based on NIST SP 800–53. The security requirements in NIST SP 800–171 are specifically tailored for use in protecting sensitive information residing in contractor information systems and generally reduce the burden placed on contractors by eliminating Federal-centric processes and requirements and enabling contractors to use systems they already have in place with some modification instead of building a new system.

Recommendations made by public comment to allow for alternative application of the rule for small entities include: An exemption for small entities, delaying application to small entities until costs are further analyzed, and creating a different set of security requirements for small entities. While all of these paths were considered, they were rejected as conflicting with the overarching purpose of this rule which is to increase the security of unclassified information that DoD has determined could result in harm if released. Regardless of the size of the contractor or subcontractor handling the information, the protection level of that information needs to be the same across the board to achieve the goal of increased information assurance.

The Chief Counsel for Advocacy of the Small Business Administration submitted a response to the second interim rule. The response reiterated the concerns brought by one of the public comments and provided suggestions for alternative application of the rule for small businesses:

Comment: The SBA Office of Advocacy suggested that DoD has underestimated the number of small businesses affected by this rulemaking, and recommended that DoD include small businesses serving as prime contractors and as subcontractors in their estimation of the number of impacted small entities. This respondent also commented that the cost of compliance with the rule will be a significant barrier to small businesses engaging in the Federal acquisition process, adding that many small businesses will be forced to purchase services and additional software from outside or third-party vendors in order to provide ''adequate safeguards'' for covered defense information and to adequately assess and evaluate their information systems and security controls.

Response: The final rule clarifies that the protections are not required when contracting solely for COTS items, thereby reducing the impact on some small business. The need to protect covered defense information does not change when such information is shared with nonfederal partners including small businesses. The cost of not protecting covered defense information is an enormous detriment to DoD resulting in a potential loss or compromise of such information, adverse impacts to the DoD warfighting mission, and to the lives of service men and women.

Comment: The SBA Office of Advocacy suggested that DoD has underestimated the number of small businesses affected by this rulemaking, and recommended that DoD include small businesses serving as prime contractors and as subcontractors in their estimation of the number of impacted small entities.

Response: As noted in response to the same public comment, DoD revises the estimate to be 12,000 small business prime contractors and any small business subcontractors that will be required to handle covered defense information during performance of the subcontracted work. There is currently no system to track when covered defense information is present on contract or passed to subcontractors so this estimate is not made with a high level of certainty.

Comment: The SBA Office of Advocacy commented that the cost of compliance with the rule will be a significant barrier to small businesses engaging in the Federal acquisition process, adding that many small businesses will be forced to purchase services and additional software from outside and third-party in order to provide ''adequate safeguards'' for covered defense information and to adequately assess and evaluate their information systems and security controls.

Response: While it is understood that implementing the minimum security controls outlined in the DFARs clause may increase costs, protection of unclassified DoD information is deemed necessary. The cost to the nation in lost intellectual property and lost technological advantage over potential adversaries is much greater than these initial/ongoing investments. The value of the information (and impact of its loss) does not diminish when it moves to contractors (prime or sub, large or small). NIST SP 800–171 was carefully crafted to use performance-based requirements and eliminate unnecessary specificity and include only those security requirements necessary to provide adequate protections for the impact level of CUI (*e.g.,* covered defense information).

Implementation of the NIST SP 800–171 security requirements will provide significant benefit to the small business community in the form of increased protection of their intellectual property. In addition, defining one set of standards will help small businesses to avoid a situation in which small business must adopt multiple standards and rule sets as they navigate amongst the many different organizations with which they do business. The addition of a new provision at DFARS 252.204–7008, Compliance with Safeguarding Covered Defense Information Controls, ensures that the offeror is aware of the requirements of clause 252.204–7012 and has time to bring their system into compliance and negotiate the terms of the contract accordingly.

Comment: The SBA Office of Advocacy suggested that DoD consider collaborating with universities or other companies, to provide low-cost cybersecurity services to small

businesses, or providing a one-time subsidy to small businesses to help cover the cost of initial consultations with third party vendors.

Response: There is no funding appropriation attached to compliance with the rule so it is not feasible to create a program for compliance or a one-time subsidy related to the new security requirements associated with the rule. However, the costs associated with compliance are allowable and should be considered in proposals on solicitations including the 252.204–7008 provision and 252.204–7012 clause, when covered defense information is present. The final rule is amended to require the security requirements to be in place only when the covered defense information is marked or identified in the contract, which should cut down significantly on the number of contractors that mistakenly assumed they were required to comply.

DoD has revised the estimate to be 12,000 small business prime contractors; however, the number of small business subcontractors that will be required to handle covered defense information during performance of the subcontracted work cannot be accurately estimated. Which small businesses will be required to comply, is entirely dependent on the work that they perform and the unclassified information involved. If they work solely in COTS items, then they will be exempt from the security requirements.

This rule requires that contractors report cyber incidents to the Government in accordance with DFARS clause 252.204–7012. An information technology expert will likely be required to provide information describing the cyber incident in the report, or at least to determine what information was affected.

For the final rule the prescriptions for provision 252.204–7008 and 252.204–7012 are amended to exempt COTS items, to clarify that they do not apply to contracts that are solely for COTS items. The final rule will keep the subcontractor flowdown requirement as amended in the second interim rule to only require the clause to flowdown when the covered defense information has been provided to the subcontractor, and this will significantly decrease the amount of small subcontractors that are unnecessarily working toward compliance with the security requirements of clause 252.204–7012.

VI. Paperwork Reduction Act

This rule contains information collection requirements that have been approved by the Office of Management and Budget (OMB) under the Paperwork Reduction Act (44 U.S.C. chapter 35) under OMB Control Number 0704–0478 entitled ''Enhanced Safeguarding and Cyber Incident Reporting of Unclassified DoD Information Within Industry.''

List of Subjects in 48 CFR Parts 202, 204, 212, 239, and 252

Government procurement.

Jennifer L. Hawes,

Editor, Defense Acquisition Regulations System.

Accordingly, the interim rule amending 48 CFR parts 202, 204, 212, 239, and 252, which was published at 80 FR 51739 on August 26, 2015, and the interim rule amending 48 CFR part 252, which was published at 80 FR 81472 on December 30, 2015, are adopted as final rules with the following changes:

■ 1. The authority citation for 48 CFR parts 202, 204, 239, and 252 continues to read as follows:

Authority: 41 U.S.C. 1303 and 48 CFR chapter 1.

PART 202—DEFINITIONS OF WORDS AND TERMS

202.101 [Amended]

■ 2. Amend section 202.101 by removing the definition of ''media''.

PART 204—ADMINISTRATIVE MATTERS

204.7300 [Amended]

■ 3. Amend section 204.7300(a) by removing ''security controls'' and adding ''security requirements'' in its place.

■ 4. Amend section 204.7301 by—

■ a. In the definition of ''covered contractor information system'', removing ''an information system'' and adding ''an unclassified information system'' in its place;

■ b. Revising the definition of ''covered defense information'';

■ c. Adding, in alphabetical order, the definition for ''media'';

■ d. Removing the definition of ''operationally critical support''; and

■ e. Amending the definition of ''rapid(ly) report(ing)'' by removing ''Rapid(ly) report(ing)'' and adding ''Rapidly report'' in its place.

The revisions and addition read as follows:

204.7301 Definitions.

* * * * *

Covered defense information means unclassified controlled technical information or other information (as described in the Controlled Unclassified Information (CUI) Registry at *http://www.archives.gov/cui/registry/category-list.html*) that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies, and is—

(1) Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract; or

(2) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract.

* * * * *

Media means physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, large-scale integration memory chips, and printouts onto which covered defense information is recorded, stored, or printed within a covered contractor information system.

* * * * *

■ 5. Amend section 204.7302 by—

■ a. Revising paragraphs (a) and (b);

■ b. In paragraph (c), removing ''The Government acknowledges that information shared by the contractor under these procedures may'' and adding ''Information shared by the contractor may'' in its place;

■ c. Revising paragraph (d); and

■ d. In paragraph (e), removing ''providing forensic analysis services, damages assessment services,'' and adding ''forensic analysis, damage assessment,'' in its place; and removing ''use and disclosure'' and adding ''use and disclosure of reported information'' in its place.

The revisions read as follows:

204.7302 Policy.

(a) Contractors and subcontractors are required to provide adequate security on all covered contractor information systems.

(b) Contractors and subcontractors are required to rapidly report cyber incidents directly to DoD at *http://dibnet.dod.mil.* Subcontractors provide the incident report number automatically assigned by DoD to the prime contractor. Lower-tier subcontractors likewise report the incident report number automatically assigned by DoD to their higher-tier subcontractor, until the prime contractor is reached.

(1) If a cyber incident occurs, contractors and subcontractors submit to DoD—

(i) A cyber incident report;

(ii) Malicious software, if detected and isolated; and

(iii) Media (or access to covered contractor information systems and equipment) upon request.

(2) Contracting officers shall refer to PGI 204.7303–4(c) for instructions on contractor submissions of media and malicious software.

* * * * *

(d) A cyber incident that is reported by a contractor or subcontractor shall not, by itself, be interpreted as evidence that the contractor or subcontractor has failed to provide adequate security on their covered contractor information systems, or has otherwise failed to meet the requirements of the clause at 252.204–7012, Safeguarding Covered Defense Information and Cyber Incident Reporting. When a cyber incident is reported, the contracting officer shall consult with the DoD component Chief Information Officer/cyber security office prior to assessing contractor compliance (see PGI 204.7303–3(a)(3)). The contracting officer shall consider such cyber incidents in the context of an overall assessment of a contractor's compliance with the requirements of the clause at 252.204–7012.

* * * * *

■ 6. Amend section 204.7304 by—

■ a. In paragraph (a), adding the phrase '', except for solicitations solely for the acquisition of commercially available off-the-shelf (COTS) items'' to the end of the sentence;

■ b. In paragraph (b), removing ''contracts for services'' and adding ''contracts, including solicitations and contracts using FAR part 12 procedures for the acquisition of commercial items, for services'' in its place; and

■ c. In paragraph (c), adding the phrase '', except for solicitations and contracts solely for the acquisition of COTS items'' to the end of the sentence.

PART 239—ACQUISITION OF INFORMATION TECHNOLOGY

■ 7. Amend section 239.7601 by adding, in alphabetical order, definitions for ''information system'' and ''media''; and removing the definition of ''spillage''.

The additions read as follows:

239.7601 Definitions.

* * * * *

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

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

■ 8. Amend section 239.7602–1 by—

■ a. In paragraph (a), removing ''the DoD'' and adding ''DoD'' in its place;

■ b. Revising paragraph (b);

■ c. In paragraph (c) introductory text, removing ''provided in the purchase request—'' and adding ''provided by the requiring activity:'' in its place;

■ d. In paragraph (c)(1), removing the semicolon and adding a period in its place;

■ e. In paragraph (c)(2), removing ''CDRL, SOW task'' and adding ''DD Form 1423, Contract Data Requirements List; work statement task;'' in its place; and removing the semicolon at the end of the second sentence and adding a period in its place;

■ f. Removing paragraphs (c)(3) and (6);

■ g. Redesignating paragraphs (c)(4) and (5) as paragraphs (c)(3) and (4);

■ h. In the newly redesignated paragraph (c)(3), removing the semicolon and adding a period in its place; and

■ i. In the newly redesignated paragraph (c)(4), removing ''litigation, eDiscovery, records management associated with the agency's retention schedules,''; and removing ''activities; and'' and adding ''activities.'' in its place.

The revision reads as follows:

239.7602–1 General.

* * * * *

(b)(1) Except as provided in paragraph (b)(2) of this section, the contracting officer shall only award a contract to acquire cloud computing services from a cloud service provider (*e.g.,* contractor or subcontractor, regardless of tier) that has been granted provisional authorization by Defense Information Systems Agency, at the level appropriate to the requirement, to provide the relevant cloud computing services in accordance with the Cloud Computing Security Requirements Guide (SRG) (version in effect at the time the solicitation is issued or as authorized by the contracting officer) found at *http://iase.disa.mil/cloud_security/Pages/index.aspx.*

(2) The contracting officer may award a contract to acquire cloud computing services from a cloud service provider that has not been granted provisional authorization when—

(i) The requirement for a provisional authorization is waived by the DoD Chief Information Officer; or

(ii) The cloud computing service requirement is for a private, on-premises version that will be provided from U.S. Government facilities. Under this circumstance, the cloud service provider must obtain a provisional authorization prior to operational use.

* * * * *

239.7602–2 [Amended]

■ 9. Amend section 239.7602–2(a) by removing ''DoD Instruction 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT)'' and adding ''DoD Instruction 8510.01'' in its place.

PART 252—SOLICITATION PROVISIONS AND CONTRACT CLAUSES

■ 10. Amend section 252.204–7000 by—

■ a. Removing the clause date of ''(AUG 2013)'' and adding ''(OCT 2016)'' in its place; and

■ b. Revising paragraph (a)(3) to read as follows:

252.204–7000 Disclosure of information.

* * * * *

(a) * * *

(3) The information results from or arises during the performance of a project that involves no covered defense information (as defined in the clause at DFARS 252.204–7012, Safeguarding Covered Defense Information and Cyber Incident Reporting) and has been scoped and negotiated by the contracting activity with the contractor and research performer and determined in writing by the contracting officer to be fundamental research (which by definition cannot involve any covered defense information), in accordance with National Security Decision Directive 189, National Policy on the Transfer of Scientific, Technical and Engineering Information, in effect on the date of contract award and the Under Secretary of Defense (Acquisition, Technology, and Logistics) memoranda on Fundamental Research, dated May 24, 2010, and on Contracted Fundamental Research, dated June 26, 2008 (available at DFARS PGI 204.4).

* * * * *

252.204–7008 [Amended]

■ 11. Amend section 252.204–7008 by—

■ a. Removing the clause date of ''(DEC 2015)'' and adding ''(OCT 2016)'' in its place;

■ b. In paragraph (a), removing ''and *covered defense information,* are'' and adding ''*covered defense information, cyber incident, information system,* and *technical information* are'' in its place.

■ c. In paragraph (b), removing ''252.204–7012, Covered Defense Information and Cyber Incident Reporting,'' and adding ''252.204–7012'' in its place;

■ d. In paragraph (c) introductory text, removing ''(IT)''; and removing ''252.204–7012(b)(1)(ii)'' and adding ''252.204–7012(b)(2)'' in its place;
■ e. In paragraph (c)(1), removing ''(see *http://dx.doi.org/10.6028/NIST.SP.800-171*),'' and adding ''(see *http://dx.doi.org/10.6028/NIST.SP.800-171*) that are in effect at the time the solicitation is issued or as authorized by the contracting officer'' in its place; and
■ f. In paragraph (c)(2)(i) introductory text, removing ''that is in effect'' and adding ''that are in effect'' in its place.

■ 12. Amend section 252.204–7009 by—
■ a. Removing the clause date of ''(DEC 2015)'' and adding ''(OCT 2016)'' in its place; and
■ b. In paragraph (a)—
■ i. Revising the definition of ''covered defense information''; and
■ ii. Adding, in alphabetical order, the definitions for ''information system'', ''media'', and ''technical information''.

The revision and additions read as follows:

252.204–7009 Limitations on the use or disclosure of third-party contractor reported cyber incident information.

* * * * *

(a) * * *

Covered defense information means unclassified controlled technical information or other information (as described in the Controlled Unclassified Information (CUI) Registry at *http://www.archives.gov/cui/registry/category-list.html*) that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies, and is—

(1) Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract; or

(2) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract.

* * * * *

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

Media means physical devices or writing surfaces including, but is not limited to, magnetic tapes, optical disks, magnetic disks, large-scale integration memory chips, and printouts onto which covered defense information is recorded, stored, or printed within a covered contractor information system.

Technical information means technical data or computer software, as those terms are defined in the clause at DFARS 252.227–7013, Rights in Technical Data—Noncommercial Items, regardless of whether or not the clause is incorporated in this solicitation or contract. Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.

* * * * *

■ 13. Amend section 252.204–7012 by—
■ a. Removing the clause date of ''(DEC 2015)'' and adding ''(OCT 2016)'' in its place;
■ b. In paragraph (a)—
■ i. Removing the definition of ''contractor information system'';
■ ii. In the definition of ''covered contractor information system'' removing ''an information system'' and adding ''an unclassified information system'' in its place;
■ iii. Revising the definition of ''covered defense information'';
■ iv. Adding, in alphabetical order, the definition for ''information system'';
■ v. In the definition of ''media'', removing ''which information is recorded'' and adding ''which covered defense information is recorded'' in its place; and removing ''within an information system'' and adding ''within a covered contractor information system'' in its place;
■ vi. In the definition of ''rapid(ly) report(ing)'', removing ''Rapid(ly) report(ing)'' and adding ''Rapidly report'' in its place; and
■ vii. In the definition of ''technical information'', removing ''Rights in Technical Data-Non Commercial Items'' and adding ''Rights in Technical Data—Noncommercial Items'' in its place;
■ c. Revising paragraph (b);
■ d. In paragraph (c)(1) introductory text, removing ''critical support'' and adding ''critical support and identified in the contract'' in its place;
■ e. Revising paragraph (d); and
■ f. Revising paragraph (m).

The revisions and addition read as follows:

252.204–7012 Safeguarding covered defense information and cyber incident reporting.

* * * * *

(a) * * *

Covered defense information means unclassified controlled technical information or other information, as described in the Controlled Unclassified Information (CUI) Registry at *http://www.archives.gov/cui/registry/category-list.html,* that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies, and is—

(1) Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract; or

(2) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract.

* * * * *

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

* * * * *

(b) *Adequate security.* The Contractor shall provide adequate security on all covered contractor information systems. To provide adequate security, the Contractor shall implement, at a minimum, the following information security protections:

(1) For covered contractor information systems that are part of an information technology (IT) service or system operated on behalf of the Government, the following security requirements apply:

(i) Cloud computing services shall be subject to the security requirements specified in the clause 252.239–7010, Cloud Computing Services, of this contract.

(ii) Any other such IT service or system (*i.e.,* other than cloud computing) shall be subject to the security requirements specified elsewhere in this contract.

(2) For covered contractor information systems that are not part of an IT service or system operated on behalf of the Government and therefore are not subject to the security requirement specified at paragraph (b)(1) of this clause, the following security requirements apply:

(i) Except as provided in paragraph (b)(2)(ii) of this clause, the covered contractor information system shall be subject to the security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800–171, ''Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations'' (available via the internet at *http://dx.doi.org/10.6028/NIST.SP.800-171*) in effect at the time the solicitation is issued or as authorized by the Contracting Officer.

(ii)(A) The Contractor shall implement NIST SP 800–171, as soon as

practical, but not later than December 31, 2017. For all contracts awarded prior to October 1, 2017, the Contractor shall notify the DoD Chief Information Officer (CIO), via email at *osd.dibcsia@mail.mil,* within 30 days of contract award, of any security requirements specified by NIST SP 800–171 not implemented at the time of contract award.

(B) The Contractor shall submit requests to vary from NIST SP 800–171 in writing to the Contracting Officer, for consideration by the DoD CIO. The Contractor need not implement any security requirement adjudicated by an authorized representative of the DoD CIO to be nonapplicable or to have an alternative, but equally effective, security measure that may be implemented in its place.

(C) If the DoD CIO has previously adjudicated the contractor's requests indicating that a requirement is not applicable or that an alternative security measure is equally effective, a copy of that approval shall be provided to the Contracting Officer when requesting its recognition under this contract.

(D) If the Contractor intends to use an external cloud service provider to store, process, or transmit any covered defense information in performance of this contract, the Contractor shall require and ensure that the cloud service provider meets security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline (*https://www.fedramp.gov/resources/documents/*) and that the cloud service provider complies with requirements in paragraphs (c) through (g) of this clause for cyber incident reporting, malicious software, media preservation and protection, access to additional information and equipment necessary for forensic analysis, and cyber incident damage assessment.

(3) Apply other information systems security measures when the Contractor reasonably determines that information systems security measures, in addition to those identified in paragraphs (b)(1) and (2) of this clause, may be required to provide adequate security in a dynamic environment or to accommodate special circumstances (*e.g.,* medical devices) and any individual, isolated, or temporary deficiencies based on an assessed risk or vulnerability. These measures may be addressed in a system security plan.

* * * * *

(d) *Malicious software.* When the Contractor or subcontractors discover and isolate malicious software in connection with a reported cyber incident, submit the malicious software to DoD Cyber Crime Center (DC3) in accordance with instructions provided by DC3 or the Contracting Officer. Do not send the malicious software to the Contracting Officer.

* * * * *

(m) *Subcontracts.* The Contractor shall—

(1) Include this clause, including this paragraph (m), in subcontracts, or similar contractual instruments, for operationally critical support, or for which subcontract performance will involve covered defense information, including subcontracts for commercial items, without alteration, except to identify the parties. The Contractor shall determine if the information required for subcontractor performance retains its identity as covered defense information and will require protection under this clause, and, if necessary, consult with the Contracting Officer; and

(2) Require subcontractors to—

(i) Notify the prime Contractor (or next higher-tier subcontractor) when submitting a request to vary from a NIST SP 800–171 security requirement to the Contracting Officer, in accordance with paragraph (b)(2)(ii)(B) of this clause; and

(ii) Provide the incident report number, automatically assigned by DoD, to the prime Contractor (or next higher-tier subcontractor) as soon as practicable, when reporting a cyber incident to DoD as required in paragraph (c) of this clause.

* * * * *

■ 14. Amend section 252.239–7010 by—

■ a. Removing the clause date of ''(AUG 2015)'' and adding ''(OCT 2016)'' in its place;

■ b. In paragraph (a)—

■ i. Adding in alphabetical order, definitions for ''compromise'' and ''information system''; and

■ ii. In the definition of ''media'', removing ''which covered defense information'' and adding ''which information'' in its place; and removing ''a covered contractor information system'' and adding ''an information system'' in its place;

■ c. In paragraph (b)(2), adding the phrase '', unless notified by the Contracting Officer that this requirement has been waived by the DoD Chief Information Officer'' to the end of the sentence; and removing the semicolon and adding a period in its place;

■ d. In paragraph (d), removing ''submitted to the Department of Defense'' and adding ''submitted to DoD'' in its place;

■ e. In paragraph (f), removing ''identified in paragraph (d) of this clause'' and adding ''identified in the cyber incident report (see paragraph (d) of this clause)'' in its place;

■ f. In paragraph (j), removing ''Local'' and adding ''local'' in its place; and

■ g. In paragraph (l), removing the phrase ''the substance of''.

The additions read as follows:

252.239–7010 Cloud computing services.

* * * * *

(a) * * *

Compromise means disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media may have occurred.

* * * * *

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

* * * * *

[FR Doc. 2016–25315 Filed 10–20–16; 8:45 am]

BILLING CODE 5001–06–P