(Billing Code 5001-06-P)

DEPARTMENT OF DEFENSE

Defense Acquisition Regulations System

48 CFR Parts 204, 212, and 252

RIN 0750-AG47

Defense Federal Acquisition Regulation Supplement: Safeguarding Unclassified Controlled Technical Information (DFARS Case 2011-D039)

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

ACTION: Final rule.

SUMMARY: DoD is issuing a final rule amending the Defense Federal Acquisition Regulation Supplement (DFARS) to add a new subpart and associated contract clause to address requirements for safeguarding unclassified controlled technical information.

DATES: *Effective* **[Insert date of publication in the FEDERAL REGISTER].**

FOR FURTHER INFORMATION CONTACT: Mr. Dustin Pitsch, Defense Acquisition Regulations System, OUSD(AT&L)DPAP/DARS, Room 3B855, 3060 Defense Pentagon, Washington, DC 20301-3060. Telephone 571-372-6090; facsimile 571-372-6101.

SUPPLEMENTARY INFORMATION:

I. Background

DoD published a proposed rule in the Federal Register at 76 FR 38089 on June 29, 2011, to implement adequate security measures to safeguard unclassified DoD information within contractor information systems from unauthorized access and disclosure, and to prescribe reporting to DoD with regard to certain cyber intrusion events that affect DoD information resident on or transiting through contractor unclassified information systems. After comments were received on the proposed rule it was decided that the scope of the rule would be modified to reduce the categories of information covered. This final rule addresses safeguarding requirements that cover only unclassified controlled technical information and reporting the compromise of unclassified controlled technical information.

Controlled technical information is technical data, computer software, and any other technical information covered by DoD Directive 5230.24, Distribution Statements on Technical Documents, at http://www.dtic.mil/whs/directives/corres/pdf/523024p.pdf, and DoD Directive 5230.25, Withholding of Unclassified Technical Data from Public Disclosure, at http://www.dtic.mil/whs/directives/corres/pdf/523025p.pdf.

Forty-nine respondents submitted public comments in response to the proposed rule.

II. Discussion and Analysis

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

A. Significant changes from the proposed rule.

- The final rule reflects changes to subpart 204.73, in lieu of 204.74 as stated in the proposed rule, to conform to the current DFARS baseline numbering sequence. Subpart 204.73 is now titled "Safeguarding Unclassified Controlled Technical Information".
- New definitions are included for: "controlled technical information", "cyber incident" and "technical information".
- These definitions published in the proposed rule are no longer included: "authentication," "clearing information," "critical program information," "cyber," "data," "DoD information," "Government information," "incident," "information," "information system," "intrusion," "nonpublic information," "safeguarding," "threat," and "voice".
- DFARS 204.7302 is modified to account for the reduced scope to limit the application of safeguarding controls to unclassified controlled technical information, which is marked in accordance with DoD Instruction 5230.24, Distribution Statements on Technical Documents.

- The "procedures" section, previously at DFARS 204.7403 in the proposed rule, is no longer included.
- DFARS 204.7303, Contract Clause, prescribes only one clause, 252.204-7012, Safeguarding of Unclassified Controlled Technical Information, which is a modification of the previously proposed "Enhanced" safeguarding clause. The previously proposed "Basic" safeguarding clause is removed and the proposed controls will be implemented through FAR case 2011-020, Basic Safeguarding of Contractor Information Systems.
- A list is added specifying the 13 pieces of information required for reporting.
- The time period a contractor must retain incident information to allow for DoD to request information necessary to conduct a damage assessment or decline interest is set at 90 days in the clause at 252.204-7012(d)(4)(iii).
- Additional information regarding DoD's damage assessment activities is added at 252.204-7012(d)(5).

B. Analysis of public comments

1. Align with implementation of Executive Order on controlled unclassified information

Comment: Numerous respondents indicated concerns that the proposed rule for DoD unclassified information was in advance of the Governmentwide guidance that the National Archives and

Records Administration is developing for controlled unclassified information (CUI). Further, they suggested that DoD delay its efforts and instead pursue alignment with the Federal CUI policy effort, in order to avoid confusion and disconnects on information categories and protections, and to prevent burdensome or duplicative costs to the contractors.

Response: To date, Federal CUI policy has not yet been promulgated for Federal Government agencies and it is unknown when Federal policy will be developed for industry as it relates to CUI. This rule has been rescoped to cover safeguarding unclassified controlled technical information, which DoD has determined to be of utmost importance and which DoD has existing authority to protect.

2. Deconflict with other policy memos, DoD Instructions (DoDI) or DoD Directives (DoDD).

Comment: Respondents suggested that the rule conflicts with policies including DoDI/DoDD 5230.24/5230.25, DoD 5000 series, DoD 8570.01-M, Directives (DoDD), National Industrial Security Operating Manual (NISPOM), DoD Information Assurance Certification and Accreditation Process (DIACAP), and Federal Information Security Management Act (FISMA).

***Response*:** The DFARS rule has been adjusted to use the marking framework established by DoDI 5230.24. DoD was unable to identify any other policy conflicts with this revised rule.

Comment: Several respondents suggested that the variety of National Institute of Standards and Technology (NIST) controls from several categories leads to a wide interpretation, which will be burdensome on personnel and there were suggestions that this hurts competition as less sophisticated firms are unable to enter the market. Another respondent suggested NIST controls should not be specified, and should be selectable by the program office. A respondent suggested that a list of controls is not sufficient and context/guidance is needed.

Response: The NIST security controls identified represent the minimum acceptable level of protection, though the clause allows for flexibility. If a control is not implemented, the contractor shall submit to the contracting officer a written explanation of how either the required security control identified is not applicable, or how an alternative control or protective measure is used to achieve equivalent protection.

Comment: Several respondents variously observed that some of the DFARS requirements are more stringent than the NISPOM.

Response: This rule has requirements to protect unclassified information stored and transmitted through unclassified networks and therefore does not align with the protection requirements in the NISPOM.

3. Policy regarding outsourcing, cloud computing, reuse, orphaned works etc.

Comment: A respondent requested clarification if use of outsourced information technology (IT) infrastructure, to include use of cloud computing, constitutes a release of information to the vendor that would be covered under the restriction on releasing information outside the Contractor's organization, and, if permitted, would the outsourced vendor be required to meet the safeguarding requirements specified in the clause.

Response: An Internet Service Provider (ISP) or cloud service provider constitutes a subcontractor in this context. The contractor is responsible for ensuring that the subcontractor complies with the requirements of this rule within the scope of this rule.

Comment: A respondent suggested the proposed rule constrains reuse of DoD information between contracts, and adds unnecessary additional DoD costs.

Response: The need-to-know requirement included in the proposed rule has been removed alleviating the concern for constraints on reuse of information. This rule is deemed necessary for the protection of unclassified controlled technical information and it is understood that implementing these controls may increase costs to DoD.

4. Consequence of noncompliance

Comment: A number of respondents commented on the lack of oversight and certification of compliance with the NIST controls in the rule.

Response: The rule does not intend to change existing penalties or remedies for noncompliance with contract requirements.

5. Government agency responsible for oversight

Comment: Two respondents suggested that the rule should identify how and by which entity audits or reviews of the safeguards will be conducted.

Response: The contract administration office is responsible for ensuring that the contractor has a process in place for meeting the required safeguarding standards. Audits or reviews will be conducted at the discretion of the contracting officer in accordance with the terms of the contract.

6. Need to clearly categorize, identify, and mark

Comment: Several respondents pointed out that DoD authority to define and mark CUI/FOUO (controlled unclassified information/for official use only) is poorly explained. FOUO is used as a catchall marking in DoD and managing this as a controlled designator is not practical. DoD is responsible for specifying a process for marking basic and enhanced criteria.

Response: The final rule has been scoped to only refer to unclassified controlled technical information. Items will be marked in accordance with DoDI 5230.24.

7. Allowable costs under Cost Accounting Standards (CAS)

Comment: One respondent asked if the cost associated with compliance to the DFARS changes is allowable under CAS.

Response: Cost Accounting Standards address measurement, allocation and assignment of costs. FAR 31 and DFARS 231, specifically FAR 31.201-2, address the allowability of costs. There is nothing in FAR 31 or DFARS 231 that would make costs of compliance with DFARS unallowable if the costs are incurred in accordance with FAR 31.201-2. While we cannot know in advance if a company will incur costs in accordance with FAR 31.201-2, there is nothing included in the final rule that would cause or compel a company to incur costs that would be in violation of FAR 31.201-2.

Comment: Several respondents stated that DoD needs to account for/provide funding for the additional costs of implementation.

Response: Implementation of this rule may increase contractor costs that would be accounted for through the normal course of business.

8. Applicability to commercial items

Comment: One respondent suggested that subcontracts for commercial items should be exempt from the unclassified data restrictions added in this rule. Several respondents suggested exempting all purchases of commercially available off-the-shelf products from the data controls added by this rule.

Response: The final rule is rescoped to focus on unclassified controlled technical information. Any unclassified controlled technical information that is shared with a contractor or subcontractor must be protected in accordance with the terms of the contract.

9. Threat sharing

Comment: A number of respondents were concerned that if the DoD did not provide threat information to companies then they would be unable to determine adequate security for the controlled information.

Response: 32 CFR part 236 provides a voluntary framework for eligible companies to exchange cyber threat information with the Government. Threat information is not needed to determine adequate security; the select NIST 800-53 controls in clause 252.204-7012, or their equivalent as suggested by the contractor, are required for adequate security. In cases where the contractor has information (either obtained from DoD or any other source) that would suggest additional security is required to adequately protect technical information, they must take action to establish that additional security.

10. Sharing of liability between the contractor and DoD

Comment: A number of respondents were concerned that the contractor will assume the full cost and liability burden for costs associated with compliance with the rule.

Response: In many cases, this contract requirement will be spread across and benefiting multiple contracts - costs associated with implementation will be allowable and chargeable to indirect cost pools. The Government does not intend to directly pay for the operating costs associated with the rule.

11. Concern for creating two types of unclassified (basic and enhanced)

Comment: A respondent indicated that, under the proposed rule, all Government unclassified information must be compartmentalized in order to effectively enforce need-to-know discipline. In addition, however, the proposed rule recognized two classes of information, one warranting "basic" protection and the second requiring "enhanced" protection. Further, the respondent indicated that the rule not only lacks clarity regarding identification and marking of the information to be protected, but also for designating the information as basic or enhanced. Additionally, the respondents recommended that uniform protocols need to be established, so documents can be sorted electronically into the proper categories.

Response: The final rule clarifies that contractors are required to protect one category of unclassified information, which was previously specified within the enhanced safeguarding clause. A proposed rule addressing “basic” safeguarding was

published in the Federal Register on Friday, August 24, 2012 (FAR 2011-020).

12. Applicability to foreign contractors

Comment: One respondent was concerned about the impact of the rule on foreign contractors and on international information sharing agreements.

Response: The technical information covered by the rule is already subject to dissemination controls that existing agreements would have to have accounted for. This rule does not have an impact on those information sharing agreements. In addition, the reporting associated with the rule is specifically focused on the information that was lost, not the cyber forensic aspects of an incident.

13. Applicability to universities

Comment: NIST SP 800-53 controls are inappropriate for academic settings and burdensome.

Response: Academic institutions dealing with unclassified controlled technical information are not exempt from the controls of this rule. The protection of the information is equally necessary, regardless of whether the contractor is a university or a business concern.

14. Scope (204.7400 redesignated 204.7300)

Comment: The respondents recommend that this rule explicitly apply to systems containing controlled information and not the general information technology environment.

Response: The rule has been revised to apply to systems that have unclassified controlled technical information resident on or transiting through them.

Comment: Several respondents made suggestions on the scope of the proposed DFARS section 204.7400 including: university fundamental research should be exempt, the rule should apply only to new contracts, the safeguards should apply to Voice over Internet Protocol (VoIP), and the protected information should be more specific and limited.

DoD will not modify the Disclosure of Information clause at DFARS 252.204-7000 in this rule. The clause at 252.204-7012 has been revised to apply to all contracts expected to be dealing with controlled technical information. Implementation of the rule does not direct modification of existing contracts. The clause does not apply to voice information, because voice information does not fall within the definition of controlled technical information.

15. Definitions (204.7401 redesignated 204.7301)

Comment: One respondent suggested adding the definition for "intrusion" at DFARS 204.7401 in addition to where it already

exists in the clause proposed at 252.204-70XX or adding a pointer to refer to the clause for definitions.

Response: The definition of "intrusion" has been deleted because the term is no longer used in the case.

16. Policy (204.7402 redesignated 204.7302)

Comment: Two respondents stated that the phrase "adequate security" and "certain cyber incidents" are too vague and need clarification. Another respondent stated that the enhanced safeguarding requirements in the clause 252.204-70YY are too stringent for unclassified information and compliance would be a substantial burden.

Response: The term "adequate security" is modified from the proposed rule to provide clarity. The final rule lays out the policy and definitions for the terms "adequate security" and "cyber incident". The criteria for reporting a cyber incident is established within the clause at 252.204-7012. DoD has determined that unclassified controlled technical information is vital to national security and must be protected.

17. Procedures

Comment: Two respondents noted that DFARS 204.7403 in the proposed rule references procedures at PGI 204.74 that were not published with the proposed rule.

Response: The "procedures" section is not included in the final rule. For future reference, when there is PGI associated with a

proposed rule, it is available at https://www.acq.osd.mil/dpap/dars/ under "Publication Notices".

18. Contract clauses (204.7404 redesignated 204.7303)

Comment: Several respondents recommended making changes to the DFARS clause prescriptions. Two respondents stated that use of "will potentially have unclassified DoD information" is vague and will result in usage errors. Two respondents recommended an exemption for fundamental research contracts; two others recommended an exemption for small businesses. One respondent stated that it is not clear if the use of 252.204-70YY negates the need for 252.204-70XX.

Response: The purpose of this rule is to protect the noted category of unclassified information, as evidenced by inclusion whenever such information would potentially be present; the best means of addressing the identified potential for usage errors is to include the clause in all contracts. The clause at DFARS 252.204-7012 is now prescribed to go in all contracts and solicitations and the additional safeguarding measures will only apply when unclassified controlled technical information is present. This change does not affect the burden placed on contractors to identify which information must be protected. The contractor's size classification is not a sufficient reason to allow a contractor to fail to protect technical information as required by clause DFARS 252.204-7012. The basic clause

previously at DFARS 252.204-70XX has been removed and will be handled as a FAR rule under FAR case 2011-020. The clause previously referred to in the proposed rule as 252.204-70YY, Enhanced Safeguarding of Unclassified DoD Information, is now at DFARS 252.204-7012. Use of this clause will not negate the use of any other clauses.

19. Clarify the Disclosure of Information clause (252.204-7000)

Comment: A number of respondents submitted comments regarding the proposed changes to clause 252.204-7000, Disclosure of Information.

Response: This final rule does not include any changes to the clause at 252.204-7000, Disclosure of Information.

20. Clarify the basic clause (proposed 252.204-70XX)

Comment: Sixteen respondents commented on concerns with the basic clause ranging from definitions, lack of specificity, and implementation issues to scope and cost burden.

Response: The basic clause, at 252.204-70XX in the proposed rule, is not included in this final rule. A basic safeguarding requirement is being developed in FAR case 2011-020.

21. Clarify the enhanced clause definitions

Comment: Eight respondents commented that the definitions for "information technology," "DoD information systems," "incident," "intrusion," "voice information," "DoD information," "non-public

information," "adequate security," and "critical program information" are too broad.

Response: Many of the definitions used in this document are from DoD standards or regulations. The definitions for "critical program information", "DoD information", "incident", "intrusion" and "nonpublic information" were removed as they were no longer necessary due to other revisions. The term "adequate security" is revised for clarity and consistency.

22. Safeguarding requirements and procedures

Comment: Four respondents requested clarification on whether DoD is requiring contractors to perform and document a specific analysis to determine if additional controls are reasonably required, or is just reconfirming that the safeguarding standards may be augmented with additional controls. They also requested clarification regarding whether a formal risk assessment is warranted by this provision, and if so, whether it will be a qualitative assessment (OCTAVE) or quantitative assessment (NIST SP-800-30). There is concern as to whether the risk assessment and proposed enhanced security measures of one contractor will be shared with other contractors or those within the Defense Industrial Base Working Group.

Response: The rule does not require a specific analysis to determine if additional controls are required. The intent is to require that if the contractor is aware, based on an already

assessed risk or vulnerability that the specified controls are inadequate, then the contractor must implement additional controls to mitigate the specific shortcoming.

Comment: A respondent questioned the provision that requires contractors with systems that do not meet the specified controls in the table to prepare a written determination that explains why the control(s) is not necessary, but only to provide the written determination to the contracting officer upon request, and suggested wording to be changed to require the determination to be included as part of their proposal.

Response: The rule has been revised to require a written explanation when the contractor intends to deviate from the specified controls. Alternative or superior safeguarding controls will not be considered as a source selection criteria.

23. DoD Information requiring enhanced safeguarding

Comment: Respondents stated that enhanced safeguards would need to be applied to all systems. Comments also indicated that DFARS should not apply to International Traffic in Arms Regulations (ITAR) and Export Administration Regulations (EAR) and information "bearing current and prior designations indicating controlled access and dissemination." ITAR and EAR are regulated by Departments of State and Commerce; other categories of information in the DFARS are already protected by

other regulations. "Critical Program Information" is poorly defined.

Response: The rule has been revised so the safeguarding requirements only apply to systems that have unclassified controlled technical information resident on or transiting through them. The rule has also been revised to specify that contractors must protect controlled technical information. Additionally, the rule ensures that there are no conflicts with existing regulations. The term "critical program information" was not included in the final rule.

Comment: A respondent noted a person communicating information requiring enhanced safeguarding would need to ensure that the recipient of that information also had a system with enhanced safeguarding, which would be challenging.

Response: The contractor has an obligation to ensure that any recipient of information requiring enhanced safeguarding is authorized to receive the information, and that it be transferred with the appropriate security. It is the responsibility of the authorized recipient to safeguard that information appropriately subject to contractual requirements.

24. Enhanced safeguarding requirements

Comment: The safeguarding controls must flow down to each subcontractor. All systems in the network would be required to meet enhanced safeguarding, increasing costs. Clarify that

enhanced safeguarding only applies to systems where DoD information resides.

Response: The enhanced safeguarding requirement only applies to systems that may have unclassified controlled technical information resident on or transiting through them.

Comment: Several respondents noted the effort and resources required of a security program that is NIST SP 800-53 compliant and the imposition of controls that are not risk based. The respondents requested that DoD consider the financial burden of applying such a security infrastructure that is more appropriate to classified than unclassified information or to more than DoD information.

Response: The rule does not require adoption of a NIST compliant security program. The rule uses the NIST SP 800-53 catalog of security controls as a reference to describe the specific security capabilities that a contractor's system should provide for enhanced safeguarding. The rule has been modified to apply only to specified controlled technical information.

Comment: A respondent recommended substantial expansion of the NIST controls listed in the table.

Response: The substantial increase in specified controls is not warranted for the sensitivity of the information being protected. Additional controls can be added to any contract when the additional security is required, but broadly applying

these additional controls is not justified or practical.

Comment: A respondent noted that the enhanced safeguarding provisions appear to expand export controls and preclude use of the fundamental research exclusion.

Response: The rule does not expand export controls and does not imply any restriction on fundamental research exclusions.

Comment: A respondent noted that there is no explicit statement that this same level of safeguarding is required for subcontractors and recommends the rule specify that the prime contractor flow down the same safeguarding requirement to each level of subcontractor.

Response: Under 252.204-7012 (g) the prime contractor is required to include the substance of this clause in all subcontracts, and each subcontractor must flow the clause down to the next tier.

Comment: Several respondents stated that the requirements for enhanced safeguarding will require contractors to implement a Common Access Card (CAC)-like public key infrastructure (PKI) system on their unclassified networks, citing NIST 800-53 controls AU-10(5) and SC-13(4), or the requirement requiring use of DoD-approved identity authentication credentials for authentication to DoD information systems.

Response: There is no requirement for contractors to implement a PKI system on their unclassified networks processing DoD

information. The NIST controls cited merely require that when using cryptography that the cryptographic algorithm meets NIST Federal Information Processing standards, or note that digital signatures can be used to ensure non-repudiation. None of the controls require PKI. If a contractor desires access to a DoD information system (one operated by or on behalf of DoD), then the authentication credentials must meet DoD standards, which typically requires a DoD-approved PKI certificate. This has been a long-standing requirement, but does not imply that the contractor system must implement PKI.

Comment: A respondent noted that the supplementary information section of the proposed rule mentions encryption of data at rest, yet the cited NIST 800-53 for protection of data at rest (SC-28) does not require encryption.

Response: The background information has been aligned in the final rule.

Comment: A respondent recommends requiring compliance with FISMA to ensure that other important FISMA requirements are met.

Response: FISMA applies only to Federal Government information and information systems or systems (or information operated or maintained by contractors on the Government's behalf). FISMA does not does not apply to the contractor information systems addressed under this rule.

Comment: A respondent comments that the rule does not establish

a clear link between the sensitivity of the information and the required level of identity assurance and suggests a set of categories for identity assurance that should be incorporated into the rule.

Response: Based on information covered by the rule, the level of identity assurance (AC or Access Control controls) specified in the clause are considered the minimum requirements.

Comment: A respondent notes that Defense Security Service requires that companies under a Foreign Ownership, Control, or Influence (FOCI)-mitigation agreement comply with certain NIST SP 800-53 requirements, the majority of which are required under this rule, leading to confusion, redundancy and wasted resources.

Response: If a company is already compliant with the NIST 800-53 controls for systems that may have unclassified controlled technical information resident on or transiting through them, then they will meet the requirements of this rule.

Comment: A respondent notes that the proposed rule is silent on prohibiting access to non-US persons, and questions whether companies (particularly those with a FOCI mitigation plan) can assume that foreign nationals and entities with a business need to know may access unclassified information unless otherwise subject to export control laws or expressly prohibited by the Government agency.

Response: This rule has no impact on existing information sharing restrictions.

25. Other requirements

Comment: One respondent was concerned about conflicting obligations under provisions of the proposed rule and recommended that participants in the Defense Industrial Base (DIB) Cyber security/information assurance (CS/IA) program be exempt from complying with the proposed rule in order to prevent the imposition of conflicting obligations.

Response: The final rule and the DIB CS/IA program Framework Agreement are mutually supportive means for safeguarding DoD information on DIB unclassified information systems. The DIB CS/IA program is voluntary and is executed under a bilateral agreement between an eligible DIB company and DoD. The DFARS language establishes contractor requirements executed under a DoD contract.

26. Cyber incident reporting

Comment: Eleven respondents commented on the requirement to report incidents within 72 hours of detection. In addition, the DFARS requires indefinite retention of forensics data for the Government and the criteria for damage assessments are broad and unclear. The respondents would like to review and comment on report content or forms prior to publication and suggested that DoD look at DSS NISPOM reporting as an option/model.

Response: The rule has been revised to clarify the reporting requirements and the timeframe for retaining data (90 days) of the potentially compromised data to support a damage assessment if the Government chooses to perform one.

27. Protection of reported information

Comment: One respondent requests the Government address how contractor incident reporting information will be protected and how it will be used. The respondent also proposed that the sharing of files and images be voluntary as it is in the Framework Agreement.

Response: Retaining files and images is an important element of the damage assessment process and is required by this rule. DoD will protect incident reporting information and any files or images in accordance with applicable statutes and regulations.

28. Third party information

Comment: Two respondents are concerned about exposure of third-party information in data provided by companies to the Government. One respondent recommended the deletion of the following: "Absent written permission, the third-party information owner may have the right to pursue legal action against the Contractor (or its subcontractors) with access to the nonpublic information for breach or unauthorized disclosure."

Response: The third party information subparagraph has been removed because support contractors working for the DoD are required to sign non-disclosure agreements. DoD personnel are bound by regulation and statute to protect proprietary information and information furnished in confidence.

29. Subcontracts

Comment: Three respondents note that the proposed rule requires the DFARS to apply to all subcontractors that may potentially have DoD information. In addition, notifications are required through the prime contractor. Potential issues exist with proprietary information and unauthorized disclosure of third party information.

Response: The rule requires that prime contractors report when unclassified controlled technical information has potentially been compromised regardless of whether the incident occurred on a prime contractor's information system or on a subcontractor's information system.

30. Provide a safe harbor for reported incidents

Comment: One respondent suggested that the rule provide explicit safe harbor in the event of a reported incident.

Response: The rule states in DFARS 204.7302(b)(2) that "A cyber incident that is properly reported by the contractor shall not, by itself, be interpreted under this clause as evidence that the contractor has failed to provide adequate information

safeguards..." The Government does not intend to provide any safe harbor statements.

31. Paperwork Burden

Comment: A number of respondents stated in various qualitative terms that the costs of compliance with the rule would be too large.

Response: The controls in the rule are taken from NIST 800-53 which closely parallels the ISO 27002 standard. As such, the controls represent mainstream industry practices. While there is cost associated with implementing information assurance controls, the use of industry practices provides assurance the costs are reasonable.

Comment: Some respondents opined that few small businesses have the basic infrastructure in place to comply and that implementation of controls would represent a larger percentage of overhead for small businesses than for large.

Response: The contractor's size classification is not a sufficient reason to allow a contractor to fail to protect technical information as required by clause 252.204-7012. The contractor at a minimum must institute the NIST (SP) 800-53 security controls identified in the table at 252.204-7012. If a control is not implemented, the contractor shall submit to the contracting officer a written explanation of how the required security control identified in the table at 252.204-7012 is not

applicable, or how an alternative control or protective measure is used to achieve equivalent protection.

Comment: Some respondents stated that the value of controls cannot be measured and that the benefits will not offset the costs.

Response: The purpose of the rule is to reduce the compromise of information. It is difficult to put a price on information and it is generally not calculated in any information protection regime. The benefits of particular controls are also difficult to quantify and further complicated by the 'arms race' dynamic of information protection. It is not possible to determine the exact point at which benefits equal costs. Nevertheless, that does not preclude taking action to protect information and accrue the associated costs.

Comment: One respondent provided an incident reporting rate of approximately 70 reports per company per year, with each report taking approximately 5 hours of company time to complete. This is in contrast to the proposed rule estimate of 0.5 incidents per company per year with a 1 hour burden per response.

Response: Since the burden estimates were estimated for the proposed rule, more data has become available, in particular from voluntary reporting by defense industrial base companies to the Defense Cyber Crime Center. Data from this voluntary program suggests five reports per company per year with a 3.5

hour burden per response. Accordingly, DoD is revising its estimate upward to five reports per company per year with a 3.5 hour burden per response.

Comment: One respondent provided a cost estimate for an appliance to capture images of auditable events of $25,000.

Response: To lower the cost of data collection in the revised rule, DoD must request the data within 90 days. Without this request, there is no obligation to retain data beyond 90 days. Image capture equates to copying the hard drive of an affected machine. The cost of media with sufficient capability to capture a hard drive image of an affected machine is in the range of $100. Assuming an average across all businesses of 12 incidents per year affecting an average of one machine and a 90 day retention period results in the ability to capture and store 3 images. 3 x $100 = $300.

32. Regulatory Flexibility Analysis

Comment: Several respondents stated that this rule will be financially burdensome for small businesses to the point that they will not be able to participate. Two respondents stated that the numbers used in the Initial Regulatory Flexibility Analysis grossly underestimate the number of businesses the rule will affect and the cost as a percentage of revenue that will be required to meet the requirements of the new rule. One respondent suggested that a gradually phased-in approach to

implement these safeguards would ease the significant financial burden they impose.

Response: This final rule was drafted with the aim of minimizing the burden of compliance on contractors while implementing the necessary safeguarding requirements.

33. Need for a public meeting

Comment: Several respondents suggested that DoD further engage the industry stakeholders, including a suggestion to schedule a public meeting to discuss the rule.

Response: Another public meeting will be considered prior to any future rules dealing with the safeguarding of information.

34. Drafting recommendations

Comment: One respondent recommends changing all instances of "unclassified Government information" to "DoD information". Several respondents submitted lists of typos and errors in the proposed rule Federal Register notice.

Response: These comments have been taken into account when drafting this final rule. The final rule uses the term "unclassified controlled technical information."

35. Out of Scope

Comment: Three respondents made comments that had no relation to the subject rule.

C. Other changes

The final rule adds a new subpart at 204.73, Safeguarding Unclassified Controlled Technical Information, to conform to the current DFARS baseline. The proposed rule had anticipated adding the new subpart at 204.74.

III. Executive Orders 12866 and 13563

Executive Orders (E.O.s) 12866 and 13563 direct agencies to assess all costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributive impacts, and equity). E.O. 13563 emphasizes the importance of quantifying both costs and benefits, of reducing costs, of harmonizing rules, and of promoting flexibility. This is a significant regulatory action and, therefore, was 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.

IV. Regulatory Flexibility Act

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

The objective of this rule is for DoD to avoid compromise of unclassified computer networks on which DoD controlled technical information is resident on or transiting through contractor

information systems, and to prevent the exfiltration of controlled technical information on such systems. The benefit of tracking and reporting DoD information compromises is to—

- Assess the impact of compromise;
- Facilitate information sharing and collaboration; and
- Standardize procedures for tracking and reporting compromise of information.

Several respondents stated that this rule will be financially burdensome for small businesses, two respondents stated that the numbers used in the Initial Regulatory Flexibility Analysis grossly underestimate the number of businesses the rule will affect and the cost as a percentage of revenue that will be required to meet the requirements of the new rule, and one respondent suggested that a gradually phased-in approach to implement these safeguards would ease the significant financial burden they impose.

No changes were made to the final rule as a result of these comments. The estimated burden in the final regulatory flexibility analysis has been reduced because the scope of the rule was modified to reduce the categories of information covered and only addresses safeguarding requirements that cover the unclassified controlled technical information and reporting the compromise of unclassified controlled technical information. The final rule is drafted with the aim of minimizing the burden

of compliance on contractors while implementing the necessary safeguarding requirements.

This final rule requires information assurance planning, including reporting of information compromise for DoD contractors that handle DoD unclassified controlled technical information. This requirement flows down to subcontracts. DoD believes that most information passed down the supply chain will not require special handling and recognizes that most large contractors handling sensitive information already have sophisticated information assurance programs and can take credit for existing controls with minimal additional cost. However, most small businesses have less sophisticated programs and will realize costs meeting the additional requirements.

Based on figures from the Defense Technical Information Center it is estimated that 6,555 contractors would be handling unclassified controlled technical information and therefore affected by this rule. Of the 6,555 contractors it is estimated that less than half of them are small entities. For the affected small entities a reasonable rule of thumb is that information technology security costs are approximately 0.5% of total revenues. Because there are economies of scale when it comes to information security, larger businesses generally pay only a fraction of that amount.

V. Paperwork Reduction Act

The rule contains information collection requirements that require the approval of the Office of Management and Budget under the Paperwork Reduction Act (44 U.S.C. chapter 35). OMB has cleared this information collection under OMB Control Number 0704-0478, titled: Defense Federal Acquisition Regulation Supplement; Safeguarding Unclassified Controlled Technical Information.

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

Government procurement.

Manuel Quinones,

Editor, Defense Acquisition Regulations System.

Therefore, 48 CFR parts 204, 212, and 252 are amended as follows:

1. The authority citation for 48 CFR parts 204, 212, and 252 continues to read as follows:

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

PART 204—ADMINISTRATIVE MATTERS

2. Add subpart 204.73 to read as follows:

Subpart 204.73—Safeguarding Unclassified Controlled Technical Information

Sec.

204.7302 Policy.

204.7303 Contract clause.

Subpart 204.73—Safeguarding Unclassified Controlled Technical Information

204.7300 Scope.

(a) This subpart applies to contracts and subcontracts requiring safeguarding of unclassified controlled technical information resident on or transiting through contractor unclassified information systems.

(b) This subpart does not abrogate any existing contractor physical, personnel, or general administrative security operations governing the protection of unclassified DoD information, nor does it impact requirements of the National Industrial Security Program.

204.7301 Definitions.

As used in this subpart—

Adequate security means protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information.

Controlled technical information means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled

technical information is to be marked with one of the distribution statements B through F, in accordance with DoD Instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions.

Cyber incident means actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein.

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-Non Commercial 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.

204.7302 Policy.

(a) DoD and its contractors and subcontractors will provide adequate security to safeguard unclassified controlled technical

information on their unclassified information systems from unauthorized access and disclosure.

(b) When safeguarding is applied to controlled technical information resident on or transiting contractor unclassified information systems—

(1) Contractors must report to DoD certain cyber incidents that affect unclassified controlled technical information resident on or transiting contractor unclassified information systems. Detailed reporting criteria and requirements are set forth in the clause at 252.204-7012, Safeguarding of Unclassified Controlled Technical Information.

(2) A cyber incident that is properly reported by the contractor shall not, by itself, be interpreted under this clause as evidence that the contractor has failed to provide adequate information safeguards for unclassified controlled technical information, or has otherwise failed to meet the requirements of the clause at 252.204-7012. When a cyber incident is reported, the contracting officer shall consult with a security manager of the requiring activity prior to assessing contractor compliance. The contracting officer shall consider such cyber incidents in the context of an overall assessment of the contractor's compliance with the requirements of the clause at 252.204-7012.

204.7303 Contract clause.

Use the clause at 252.204-7012, Safeguarding of Unclassified Controlled Technical Information, in all solicitations and contracts, including solicitations and contracts using FAR part 12 procedures for the acquisition of commercial items.

PART 212—ACQUISITION OF COMMERCIAL ITEMS

3. Section 212.301 is amended by—

a. Redesignating paragraphs (f)(vi) through (lxvii) as (vii) through (lxviii); and

b. Adding new paragraph (f)(vi) to read as follows:

212.301 Solicitation provisions and contract clauses for the acquisition of commercial items.

(f) * * *

(vi) Use the clause at 252.204-7012, Safeguarding of Unclassified Controlled Technical Information, as prescribed in 204.7303.

* * * * *

PART 252—SOLICITATION PROVISIONS AND CONTRACT CLAUSES

4. Add section 252.204-7012 to read as follows:

252.204-7012 Safeguarding of unclassified controlled technical information.

As prescribed in 204.7303, use the following clause:

SAFEGUARDING OF UNCLASSIFIED CONTROLLED TECHNICAL INFORMATION (NOV 2013)

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

Adequate security means protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information.

Attribution information means information that identifies the Contractor, whether directly or indirectly, by the grouping of information that can be traced back to the Contractor (e.g., program description or facility locations).

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.

Contractor information system means an information system belonging to, or operated by or for, the Contractor.

Controlled technical information means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information is to be marked with one of the distribution statements B-through-F, in accordance with DoD Instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions.

Cyber incident means actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein.

Exfiltration means any unauthorized release of data from within an information system. This includes copying the data through covert network channels or the copying of data to unauthorized media.

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 information is recorded, stored, or printed within an 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-Non Commercial 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.

(b) *Safeguarding requirements and procedures for unclassified controlled technical information*. The Contractor shall provide adequate security to safeguard unclassified controlled technical information from compromise. To provide adequate security, the Contractor shall—

(1) Implement information systems security in its project, enterprise, or company-wide unclassified information technology system(s) that may have unclassified controlled technical information resident on or transiting through them. The information systems security program shall implement, at a minimum—

(i) The specified National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 security controls identified in the following table; or

(ii) If a NIST control is not implemented, the Contractor shall submit to the Contracting Officer a written explanation of how—

(A) The required security control identified in the following table is not applicable; or

(B) An alternative control or protective measure is used to achieve equivalent protection.

(2) Apply other information systems security requirements when the Contractor reasonably determines that information systems security measures, in addition to those identified in

paragraph (b)(1) of this clause, may be required to provide adequate security in a dynamic environment based on an assessed risk or vulnerability.

Table 1 -- Minimum Security Controls for Safeguarding

Minimum required security controls for unclassified controlled technical information requiring safeguarding in accordance with paragraph (d) of this clause. (A description of the security controls is in the NIST SP 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations" (http://csrc.nist.gov/publications/PubsSPs.html).)

Access Control	Audit & Accountability	Identification and Authentication	Media Protection	System & Comm Protection
AC-2	AU-2	IA-2	MP-4	SC-2
AC-3(4)	AU-3	IA-4	MP-6	SC-4
AC-4	AU-6(1)	IA-5(1)		SC-7
			Physical and Environmental Protection	
AC-6	AU-7			SC-8(1)
		Incident Response		
AC-7	AU-8		PE-2	SC-13
AC-11(1)	AU-9	IR-2	PE-3	
AC-17(2)		IR-4	PE-5	SC-15
	Configuration Management			
AC-18(1)		IR-5		SC-28
			Program Management	
AC-19	CM-2	IR-6		
				System & Information Integrity
AC-20(1)	CM-6		PM-10	
AC-20(2)	CM-7	Maintenance		SI-2
AC-22	CM-8	MA-4(6)	Risk Assessment	SI-3
		MA-5	RA-5	SI-4
Awareness & Training	Contingency Planning			
AT-2	CP-9	MA-6		

Legend:

AC:	Access Control	MA:	Maintenance
AT:	Awareness and Training	MP:	Media Protection
AU:	Auditing and Accountability	PE:	Physical & Environmental Protection
CM:	Configuration Management	PM:	Program Management
CP:	Contingency Planning	RA:	Risk Assessment
IA:	Identification and Authentication	SC:	System & Communications Protection
IR:	Incident Response	SI:	System & Information Integrity

(c) *Other requirements*. This clause does not relieve the Contractor of the requirements specified by applicable statutes or other Federal and DoD safeguarding requirements for Controlled Unclassified Information as established by Executive Order 13556, as well as regulations and guidance established pursuant thereto.

(d) *Cyber incident and compromise reporting*.

(1) *Reporting requirement*. The Contractor shall report as much of the following information as can be obtained to the Department of Defense via (http://dibnet.dod.mil/) within 72 hours of discovery of any cyber incident, as described in

paragraph (d)(2) of this clause, that affects unclassified controlled technical information resident on or transiting through the Contractor's unclassified information systems:

(i) Data Universal Numbering System (DUNS).

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

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

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

(v) Contracting Officer point of contact (address, position, telephone, email).

(vi) Contract clearance level.

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

(viii) DoD programs, platforms or systems involved.

(ix) Location(s) of compromise.

(x) Date incident discovered.

(xi) Type of compromise (e.g., unauthorized access, inadvertent release, other).

(xii) Description of technical information compromised.

(xiii) Any additional information relevant to the information compromise.

(2) *Reportable cyber incidents*. Reportable cyber incidents include the following:

(i) A cyber incident involving possible exfiltration, manipulation, or other loss or compromise of any unclassified controlled technical information resident on or transiting through Contractor's, or its subcontractors', unclassified information systems.

(ii) Any other activities not included in paragraph (d)(2)(i) of this clause that allow unauthorized access to the Contractor's unclassified information system on which unclassified controlled technical information is resident on or transiting.

(3) *Other reporting requirements*. This reporting in no way abrogates the Contractor's responsibility for additional safeguarding and cyber incident reporting requirements pertaining to its unclassified information systems under other clauses that may apply to its contract, or as a result of other U.S. Government legislative and regulatory requirements that may apply (e.g., as cited in paragraph (c) of this clause).

(4) *Contractor actions to support DoD damage assessment*. In response to the reported cyber incident, the Contractor shall—

(i) Conduct further review of its unclassified network for evidence of compromise resulting from a cyber incident to

include, but is not limited to, identifying compromised computers, servers, specific data and users accounts. This includes analyzing information systems that were part of the compromise, as well as other information systems on the network that were accessed as a result of the compromise;

(ii) Review the data accessed during the cyber incident to identify specific unclassified controlled technical information associated with DoD programs, systems or contracts, including military programs, systems and technology; and

(iii) Preserve and protect images of known affected information systems and all relevant monitoring/packet capture data for at least 90 days from the cyber incident to allow DoD to request information or decline interest.

(5) *DoD damage assessment activities*. If DoD elects to conduct a damage assessment, the Contracting Officer will request that the Contractor point of contact identified in the incident report at (d)(1) of this clause provide all of the damage assessment information gathered in accordance with paragraph (d)(4) of this clause. The Contractor shall comply with damage assessment information requests. The requirement to share files and images exists unless there are legal restrictions that limit a company's ability to share digital media. The Contractor shall inform the Contracting Officer of

the source, nature, and prescription of such limitations and the authority responsible.

(e) *Protection of reported information*. Except to the extent that such information is lawfully publicly available without restrictions, the Government will protect information reported or otherwise provided to DoD under this clause in accordance with applicable statutes, regulations, and policies. The Contractor shall identify and mark attribution information reported or otherwise provided to the DoD. The Government may use information, including attribution information and disclose it only to authorized persons for purposes and activities consistent with this clause.

(f) Nothing in this clause limits the Government's ability to conduct law enforcement or counterintelligence activities, or other lawful activities in the interest of homeland security and national security. The results of the activities described in this clause may be used to support an investigation and prosecution of any person or entity, including those attempting to infiltrate or compromise information on a contractor information system in violation of any statute.

(g) *Subcontracts*. The Contractor shall include the substance of this clause, including this paragraph (g), in all subcontracts, including subcontracts for commercial items.

(End of clause)

[FR Doc. 2013-27313 Filed 11/15/2013 at 8:45 am; Publication Date: 11/18/2013]