DEPARTMENT OF DEFENSE **BILLING CODE 5001-06**

Office of the Secretary

32 CFR Part 236

[DOD-2014-OS-0097]

RIN 0790-AJ29

Department of Defense (DoD)-Defense Industrial Base (DIB) Cybersecurity (CS) Activities

AGENCY: Office of the DoD Chief Information Officer, DoD.

ACTION: Interim final rule.

SUMMARY: DoD is revising its DoD-DIB Cybersecurity (CS) Activities regulation to mandate reporting of cyber incidents that result in an actual or potentially adverse effect on a covered contractor information system or covered defense information residing therein, or on a contractor's ability to provide operationally critical support, and modify eligibility criteria to permit greater participation in the voluntary DoD-Defense Industrial Base (DIB) Cybersecurity (CS) information sharing program.

DATES: Effective Date: This rule if effective [INSERT DATE OF PUBLICATION IN THE FEDERAL REGISTER. Comments must be received by [INSERT 60 DAYS FROM DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: You may submit comments, identified by docket number and/or Regulatory Information Number (RIN) number and title, by any of the following methods:

- Federal Rulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments.

Mail: Department of Defense, Office of the Deputy Chief Management Officer, Directorate of Oversight and Compliance, Regulatory and Audit Matters Office, 9010 Defense Pentagon, Washington, DC 20301-9010.

FOR FURTHER INFORMATION CONTACT: DoD-DIB Cybersecurity Activities Office: (703) 604-3167, toll free (855) 363-4227.

SUPPLEMENTARY INFORMATION:

Executive Summary

This rule revises the DoD-DIB cybersecurity information sharing program regulation to implement new statutory requirements for DoD contractors and subcontractors to report cyber incidents that result in an actual or potentially adverse effect on a covered contractor information system or covered defense information residing therein, or on a contractor's ability to provide operationally critical support. The program also retains the voluntary information sharing activities for cybersecurity information that is outside the scope of the mandatory reporting requirements.

Regarding the mandatory reporting, this part has been revised to set forth mandatory cyber incident reporting requirements that will apply to all forms of contracts or other agreements between DoD and DIB companies (e.g., procurement contracts, cooperative agreements, other transaction agreements). Thus, all relevant contracts or agreements are required to include these cyber reporting requirements (e.g., through incorporation of the reporting requirements by reference, or by expressly setting forth reporting requirements consistent with this part). The revisions provided in this rule are part of DoD's efforts to establish a single reporting mechanism for such cyber incidents on unclassified DoD contractor information systems. These requirements are focused on cyber incidents that threaten specific types of DoD program

information, such as technical information controlled under the International Traffic in Arms Regulations or the Export Administration Regulations or otherwise controlled by DOD and operational security information that relates to DoD activities. Additional cyber incident reporting requirements for other important types of controlled unclassified information (CUI) (e.g., personally identifiable information (PII), budget or financial information) are more specifically addressed through other regulatory mechanisms, and thus are outside the scope of this rule. To clarify this distinction, the rule explicitly states that reporting under this program does not abrogate the contractor's responsibility for any other applicable cyber incident reporting requirements (§ 236.4(o)).

The rule also revises the program's definitions to better harmonize with definitions that are already established and used by DoD and other Government agencies in similar contexts, such as those relating to the handling and safeguarding of Controlled Unclassified Information as used by the National Archives and Records Administration pursuant to Executive Order 13556 "Controlled Unclassified Information" (November 4, 2010) (see http://www.archives.gov/cui/), and those widely used in the context of cybersecurity activities (see the Committee on National Security Systems Instruction No. 4009, "National Information Assurance Glossary").

This rule is intended to streamline the reporting process for DoD contractors and minimize duplicative reporting processes, while preserving distinctions where appropriate. Cyber incident reporting involving classified information on classified contractor systems will be in accordance with the National Industrial Security Program Operating Manual (DoD-M 5220.22 (http://www.dtic.mil/whs/directives/corres/pdf/522022m.pdf)).

This rule also modifies eligibility criteria to permit greater participation in the voluntary DoD-DIB CS information sharing program. Expanding participation in the DoD-DIB CS information

sharing program is part of DoD's comprehensive approach to counter cyber threats through information sharing between the Government and DIB participants. The DoD-DIB CS information sharing program allows eligible DIB participants to receive Government furnished information (GFI) and cyber threat information from other DIB participants, thereby providing greater insights into adversarial activity targeting the DIB. The activities in this rule implement DoD statutory authorities to establish programs and activities to protect sensitive DoD information, including when such information resides on or transits information systems operated by contractors or others in support of DoD activities (e.g., 10 U.S.C. 391 and 2224, the Federal Information Security Modernization Act (FISMA), codified at 44 U.S.C. 3551 *et seq*., section 941 of the NDAA for FY 2013 (Public Law 112-239)). Activities under this rule also fulfill important elements of DoD's critical infrastructure protection responsibilities, as the sector specific agency for the DIB sector (see Presidential Policy Directive 21 (PPD-21), "Critical Infrastructure Security and Resilience," available at https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil). Under this rule, contractors will incur costs associated with requirements for reporting cyber incidents of covered defense information on their covered contractor information system(s) or those affecting the contractor's ability to provide operationally critical support. Costs for contractors include identifying and analyzing cyber incidents and their impact on covered defense information, or a contractor's ability to provide operationally critical support, as well as obtaining DoD-approved medium assurance certificates to ensure authentication and identification when reporting cyber incidents to DoD. Government costs include onboarding new companies under the voluntary DoD-DIB CS information sharing program, and collecting and analyzing cyber incident reports, malicious software, and media.

A foundational element of these new mandatory reporting requirements, as well as the voluntary DoD-DIB CS information sharing activities, is the recognition that the information being shared between the parties includes extremely sensitive information that requires protection.

For additional information regarding the Government's safeguarding of information received from the contractors that require protection, see the Privacy Impact Assessment (PIA) for the DIB Cybersecurity/Information Assurance Activities located at http://dodcio.defense.gov/Portals/0/Documents/DIB%20CS-IA%20PIA_FINAL_signed_30jun2011_VMSS_GGMR_RC.pdf. The PIA provides detailed procedures for handling personally identifiable information (PII), attributional information about the strengths or vulnerabilities of specific covered contractor information systems, information providing a perceived or real competitive advantage on future procurement action, and contractor information marked as proprietary or commercial or financial information.

Interim Final Rule Justification

This rule is being published as an interim rule in order to comply with statutory guidance under Section 941 of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2013, and section 391 of Title 10, United States Code (U.S.C.), requiring defense contractors to rapidly report cyber incidents on their unclassified networks or information systems that may affect unclassified defense information, or that affect their ability to provide operationally critical support to the Department. Issuing this rule as an interim final rule underscores the importance of better protecting unclassified defense information against the immediate cyber threat, while preserving the intellectual property and competitive capabilities of our national defense industrial base. The interim final rule enables DoD to better assess, in the near term, when mission critical capabilities and services are affected by cyber incidents and reinforces DoD's overall efforts to

defend DoD information, protect U.S. national interests against cyber-attacks, and support military operations and contingency plans worldwide. Cybersecurity is a Congressional priority and this interim final rule supports the Administration's national cybersecurity strategy emphasizing public-private information sharing.

Regulatory Procedures

Executive Orders 12866, "Regulatory Planning and Review" and 13563, "Improving Regulation and Regulatory Review"

Executive Orders 13563 and 12866 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, distribute impacts, and equity). Executive Order 13563 emphasizes the importance of quantifying both costs and benefits, of reducing costs, of harmonizing rules, and of promoting flexibility. This rule has been designated a "significant regulatory action," although not economically significant, under section 3(f) of Executive Order 12866. Accordingly, the rule has been reviewed by the Office of Management and Budget (OMB).

Public Law 104-121, "Congressional Review Act" (5 U.S.C. 801)

It has been determined that this rule is not a "major" rule under 5 U.S.C. 801, enacted by Public Law 104-121, because it will not result in an annual effect on the economy of $100 million or more; a major increase in costs or prices for consumers, individual industries, Federal, State, or local Government agencies, or geographic regions; or significant adverse effects on competition, employment, investment, productivity, innovation, or on the ability of United States-based enterprises to compete with foreign-based enterprises in domestic and export markets.

Sec. 202, Public Law 104-4, "Unfunded Mandates Reform Act"

It has been determined that this rule does not contain a Federal mandate that may result in expenditure by State, local and tribal Governments, in aggregate, or by the private sector, of $100 million or more in any one year.

Public Law 96-354, "Regulatory Flexibility Act" (5 U.S.C. 601)

It has been certified that this rule is not subject to the Regulatory Flexibility Act (5 U.S.C. 601) because it would not, if promulgated, have a significant economic impact on a substantial number of small entities. Therefore, the Regulatory Flexibility Act, as amended, does not require us to prepare a regulatory flexibility analysis.

Public Law 96-511, "Paperwork Reduction Act" (44 U.S.C. Chapter 35)

It has been determined that 32 CFR part 236 does contain reporting or recordkeeping requirements under the Paper Reduction Act (PRA) of 1995. These reporting requirements apply existing collection approvals under Office of Management and Budget (OMB) Control Numbers: 0704-0489, "Defense Industrial Base Cyber Security/Information Assurance (DIB CS/IA) Cyber Incident Reporting," and 0704-0490, "Defense Industrial Base Cyber Security/Information Assurance (DIB CS/IA) Points of Contact (POC) Information."

DoD has submitted a revision for the 0704-0489 collection to OMB under the provisions of the Paperwork Reduction Act (44 U.S.C. Chapter 35) in response to 32 CFR part 236 expanding the number of companies under mandatory cyber incident reporting requirements. Comments are invited on: (a) whether the proposed collection of information is necessary for the proper performance of the functions of DoD, including whether the information will have practical utility; (b) the accuracy of the estimate of the burden of the proposed information collection; (c)

ways to enhance the quality, utility, and clarity of the information to be collected; and (d) ways to minimize the burden of the information collection on respondents, including the use of automated collection techniques or other forms of information technology.

Title: Cyber Incident Reporting by DoD Contractors

Type of Request: Revision.

Number of DoD contractors impacted is 10,000

Projected Responses Per Participant Per Year: 5

Annual Total Responses: Up to 50,000

Average Burden Per Response: 7 hours (this includes searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information).

Annual Total Burden Hours: 250,000 hours for all participants

Needs and Uses: The requested information supports the mandatory cyber incident reporting requirements under Section 941 of the NDAA for Fiscal Year (FY) 13 and Section 1632 of the NDAA for FY 15, and facilitates cyber situational awareness and cyber threat information sharing. DoD contractors report incidents using the standard Incident Collection Format (ICF). The primary means of reporting is through a secure unclassified web portal, but a company may report incidents through other communication means if necessary.

Affected Public: DoD contractors with the provisions of 32 CFR part 236 in their agreements with DoD.

Frequency: On occasion.

Respondent's Obligation: Mandatory

DoD has submitted a revision for the 0704-0490 collection to OMB under the provisions of the Paperwork Reduction Act (44 U.S.C. Chapter 35) in response to 32 CFR part 236 expanding

the number of companies eligible to participate in the voluntary DIB CS information sharing program. Comments are invited on: (a) whether the proposed collection of information is necessary for the proper performance of the functions of DoD, including whether the information will have practical utility; (b) the accuracy of the estimate of the burden of the proposed information collection; (c) ways to enhance the quality, utility, and clarity of the information to be collected; and (d) ways to minimize the burden of the information collection on respondents, including the use of automated collection techniques or other forms of information technology.

Title: Defense Industrial Base Cybersecurity Activities Points of Contact (POC) Information

Type of Request: Revision.

Number of DoD contractors impacted is 8,500. DoD estimates that no more than 10% of the total eligible population of cleared defense contractors will apply to the voluntary DIB Cybersecurity Activities program resulting in 850 cleared defense contractors impacted annually. An additional 10% of the population or 85 contractors may provide updated points of contact for the program, as required.

Projected Responses Per Participant: Initial collection is one per company with updates on a case-by-case basis.

Annual Total Responses: 935

Average Burden Per Response: 20 minutes.

Annual Total Burden Hours: 312 hours for all participants

Needs and Uses: The Government will collect business points of contact (POC) information from all Defense Industrial Base (DIB) Cybersecurity program participants on a one-time basis, with updates as necessary, to facilitate communications and the sharing of share unclassified and classified cyber threat information.

Affected Public: Business or other for-profit and not-for-profit institutions.

Frequency: On occasion.

Respondent's Obligation: Voluntary.

OMB Desk Officer:

Written comments and recommendations on these information collections should be sent to Ms. Jasmeet Seehra at the Office of Management and Budget, DoD Desk Officer, Room 10102, New Executive Office Building, Washington, DC 20503, with a copy to the Director, DoD-DIB Cybersecurity Activities Office, at the Office of the DoD Chief Information Officer, 6000 Defense Pentagon, Attn: DIB CS Activities Office, Washington, D.C. 20301-6000, or email at OSD.DIBCSIA@mail.mil.

You may also submit comments, identified by docket number and title, by the following method:

Federal Rulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments.

All submissions received must include the agency name, docket number and title for this Federal Register document. The general policy for comments and other submissions from members of the public is to make these submissions available for public viewing on the Internet at http://www.regulations.gov as they are received without change, including any personal identifiers or contact information.

Executive Order 13132, "Federalism"

It has been determined that this rule does not have federalism implications, as set forth in Executive Order 13132. This rule does not have substantial direct effects on:

(a) The States;

(b) The relationship between the National Government and the States; or

(c) The distribution of power and responsibilities among the various levels of Government.

List of Subjects in 32 CFR Part 236

Government contracts, Security measures.

Accordingly, 32 CFR part 236 is revised to read as follows:

PART 236– DEPARTMENT OF DEFENSE (DoD)-DEFENSE INDUSTRIAL BASE (DIB) CYBERSECURITY (CS) ACTIVITIES

Sec.

Authority: 10 U.S.C. 391; 10 U.S.C. 2224; 44 U.S.C. 3506; 44 U.S.C. 3544; and Section 941, Public Law 112–239, 126 Stat. 1632.

§236.1 Purpose.

Cyber threats to contractor unclassified information systems represent an unacceptable risk of compromise of DoD information and pose an imminent threat to U.S. national security and economic security interests. This part requires all DoD contractors to rapidly report cyber incidents involving covered defense information on their covered contractor information systems

or cyber incidents affecting the contractor's ability to provide operationally critical support. The part also modifies the eligibility criteria to permit greater participation in the voluntary DoD-DIB CS information sharing program in which DoD provides cyber threat information and cybersecurity best practices to DIB participants. The DoD-DIB CS information sharing program enhances and supplements DIB participants' capabilities to safeguard DoD information that resides on, or transits, DIB unclassified information systems.

§236.2 Definitions.

As used in this part:

Access to media means provision of media, or access to media physically or remotely to DoD personnel, as determined by the contractor.

Cleared defense contractor (CDC) means a private entity granted clearance by DoD to access, receive, or store classified information for the purpose of bidding for a contract or conducting activities in support of any program of DoD.

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 means an individual or organization outside the U.S. Government who has accepted any type of agreement or order to provide research, supplies, or services to DoD, including prime contractors and subcontractors.

Contractor attributional/proprietary information means information that identifies the contractor(s), whether directly or indirectly, by the grouping of information that can be traced back to the contractor(s) (e.g., program description, facility locations), personally identifiable information, as well

as trade secrets, commercial or financial information, or other commercially sensitive information that is not customarily shared outside of the company.

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 would meet the criteria, if disseminated, for distribution statements B through F using the criteria set forth in DoD Instruction 5230.24, "Distribution Statements of Technical Documents," available at http://www.dtic.mil/whs/directives/corres/pdf/523024p.pdf. The term does not include information that is lawfully publicly available without restrictions.

Covered contractor information system means an information system that is owned or operated by or for a contractor and that processes, stores, or transmits covered defense information.

Covered defense information means unclassified information that:

(1) Is:

(i) Provided to the contractor by or on behalf of the DoD in connection with the performance of a contract; or

(ii) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of a contract; and

(2) Falls in any of the following categories:

(i) Controlled Technical Information;

(ii) Critical information (operations security). Specific facts identified through the Operations Security process about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment (part of Operations Security process);

(iii) Export Control. Unclassified information concerning certain items, commodities, technology, software, or other information whose export could reasonably be expected to adversely affect the United States national security and nonproliferation objectives. To include dual use items; items identified in export administration regulations, international traffic in arms regulations and munitions list; license applications; and sensitive nuclear technology information;

(iv) Any other information, marked or otherwise identified by the Government, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies (e.g., privacy, proprietary business information).

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

Cyber incident damage assessment means a managed, coordinated process to determine the effect on defense programs, defense scientific and research projects, or defense warfighting capabilities resulting from compromise of a contractor's unclassified computer system or network.

Defense Industrial Base (DIB) means the Department of Defense, Government, and private sector worldwide industrial complex with capabilities to perform research and development, design, produce, and maintain military weapon systems, subsystems, components, or parts to satisfy military requirements.

DIB participant means a CDC that has met all of the eligibility requirements to participate in the voluntary DoD-DIB CS Information Sharing Program as set forth in this part (see § 236.7).

Forensic analysis means the practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data.

Government furnished information (GFI) means information provided by the Government under the voluntary DoD-DIB CS information sharing program including but not limited to cyber threat information and cybersecurity practices.

Information means any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.

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

Malicious software means software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. This definition includes a virus, worm, Trojan horse, or other code-based entity that infects a host, as well as spyware and some forms of adware.

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.

Operationally critical support means supplies or services designated by the Government as critical for airlift, sealift, intermodal transportation services, or logistical support that is essential to the mobilization, deployment, or sustainment of the Armed Forces in a contingency operation.

Rapid(ly) report(ing) means within 72 hours of discovery of any cyber incident.

Technical Information means technical data or computer software, as those terms are defined in

DFARS 252.227-7013, "Rights in Technical Data—Noncommercial Items" (48 CFR 252.227-7013). 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.

Threat means any circumstance or event with the potential to adversely impact organization operations (including mission, functions, image, or reputation), organization assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information and/or denial of service.

U.S. based means provisioned, maintained, or operated within the physical boundaries of the United States.

U.S. citizen means a person born in the United States or naturalized.

§236.3 Policy.

It is DoD policy to:

(a) Establish a comprehensive approach to require safeguarding of covered defense information on covered contractor information systems and to require contractor cyber incident reporting.

(b) Increase Government stakeholder and DIB situational awareness of the extent and severity of cyber threats to DoD information by implementing a streamlined approval process that enables the contractor to elect, in conjunction with the cyber incident reporting and sharing, the extent to which DoD may share cyber threat information obtained from a contractor (or derived from information obtained from the company) under this part that is not information created by or for DoD with:

(1) DIB contractors participating in the DoD-DIB CS information sharing program to enhance their cybersecurity posture to better protect covered defense information on covered contractor information systems, or a contractor's ability to provide operationally critical support; and

(2) Other Government stakeholders for lawful Government activities, including cybersecurity for the protection of Government information or information systems, law enforcement and counterintelligence (LE/CI), and other lawful national security activities directed against the cyber threat (e.g., those attempting to infiltrate and compromise information on the contractor information systems).

(c) Modify eligibility criteria to permit greater participation in the voluntary DoD-DIB CS information sharing program.

§236.4 Mandatory cyber incident reporting procedures.

(a) *Applicability and order of precedence*. The requirement to report cyber incidents shall be included in all applicable agreements between the Government and the contractor in which covered defense information resides on, or transits covered contractor information systems or under which a contractor provides operationally critical support, and shall be identical to those requirements provided in this section (e.g., by incorporating the requirements of this section by reference, or by expressly setting forth such reporting requirements consistent with those of this section). Any inconsistency between the relevant terms and condition of any such agreement and this section shall be resolved in favor of the terms and conditions of the agreement, provided and to the extent that such terms and conditions are authorized to have been included in the agreement in accordance with applicable laws and regulations.

(b) *Cyber incident reporting requirement*. When a contractor discovers a cyber incident that affects a covered contractor information system or the covered defense information residing

therein or that affects the contractor's ability to provide operationally critical support, the contractor shall:

(1) Conduct a review for evidence of compromise of covered defense information including, but not limited to, identifying compromised computers, servers, specific data, and user accounts. This review shall also include analyzing covered contractor information system(s) that were part of the cyber incident, as well as other information systems on the contractor's network(s), that may have been accessed as a result of the incident in order to identify compromised covered defense information, or that affect the contractor's ability to provide operationally critical support; and

(2) Rapidly report cyber incidents to DoD at http://dibnet.dod.mil.

(c) *Cyber incident report*. The cyber incident report shall be treated as information created by or for DoD and shall include, at a minimum, the required elements at http://dibnet.dod.mil.

(d) *Subcontractor reporting procedures.* Contractors shall flow down the cyber incident reporting requirements of this part to their subcontractors, as appropriate. Contractors shall require subcontractors to rapidly report cyber incidents directly to DoD at http://dibnet.dod.mil and the prime contractor. This includes providing the incident report number, automatically assigned by DoD, to the prime contractor (or next higher-tier subcontractor) as soon as practicable.

(e) *Medium assurance certificate requirement.* In order to report cyber incidents in accordance with this part, the contractor or subcontractor shall have or acquire a DoD-approved medium assurance certificate to report cyber incidents. For information on obtaining a DoD-approved medium assurance certificate, see http://iase.disa.mil/pki/eca/certificate.html.

(f) If the contractor utilizes a third-party service provider (SP) for information system security services, the SP may report cyber incidents on behalf of the contractor.

(g) Contractors are encouraged to report information to promote sharing of cyber threat indicators that they believe are valuable in alerting the Government and others, as appropriate in order to better counter threat actor activity. Cyber incidents that are not compromises of covered defense information or do not adversely affect the contractor's ability to perform operationally critical support may be of interest to the DIB and DoD for situational awareness purposes.

(h) *Malicious software.* Malicious software discovered and isolated by the contractor will be submitted to the DoD Cyber Crime Center (DC3) for forensic analysis.

(i) *Media preservation and protection.* When a contractor discovers a cyber incident has occurred, the contractor shall preserve and protect images of known affected information systems identified in paragraph (b) of this section and all relevant monitoring/packet capture data for at least 90 days from submission of the cyber incident report to allow DoD to request the media or decline interest.

(j) *Access to additional information or equipment necessary for forensics analysis.* Upon request by DoD, the contractor shall provide DoD with access to additional information or equipment that is necessary to conduct a forensic analysis.

(k) *Cyber incident damage assessment activities.* If DoD elects to conduct a damage assessment, DoD will request that the contractor provide all of the damage assessment information gathered in accordance with paragraph (e) of this section.

(l) *DoD safeguarding and use of contractor attributional/proprietary information.* The Government shall protect against the unauthorized use or release of information obtained from the contractor (or derived from information obtained from the contractor) under this part that

includes contractor attributional/proprietary information, including such information submitted in accordance with paragraph (b) of this section. To the maximum extent practicable, the contractor shall identify and mark attributional/proprietary information. In making an authorized release of such information, the Government will implement appropriate procedures to minimize the contractor attributional/proprietary information that is included in such authorized release, seeking to include only that information that is necessary for the authorized purpose(s) for which the information is being released.

(m) *Use and release of contractor attributional/proprietary information not created by or for DoD.* Information that is obtained from the contractor (or derived from information obtained from the contractor) under this part that is not created by or for DoD is authorized to be released outside of DoD:

(1) To entities with missions that may be affected by such information;

(2) To entities that may be called upon to assist in the diagnosis, detection, or mitigation of cyber incidents;

(3) To Government entities that conduct LE/CI investigations;

(4) For national security purposes, including cyber situational awareness and defense purposes (including sharing with DIB contractors participating in the DIB CS program authorized by this part); or

(5) To a support services contractor ("recipient") that is directly supporting Government activities related to this part and is bound by use and non-disclosure restrictions that include all of the following conditions:

(i) The recipient shall access and use the information only for the purpose of furnishing advice or technical assistance directly to the Government in support of the Government's activities related to this part, and shall not be used for any other purpose;

(ii) The recipient shall protect the information against unauthorized release or disclosure;

(iii) The recipient shall ensure that its employees are subject to use and non-disclosure obligations consistent with this part prior to the employees being provided access to or use of the information;

(iv) The third-party contractor that reported the cyber incident is a third-party beneficiary of the non-disclosure agreement between the Government and the recipient, as required by paragraph (m)(5)(iii) of this section;

(v) That a breach of these obligations or restrictions may subject the recipient to:

(A) Criminal, civil, administrative, and contractual actions in law and equity for penalties, damages, and other appropriate remedies by the United States; and

(B) Civil actions for damages and other appropriate remedies by the third party that reported the incident, as a third party beneficiary of the non-disclosure agreement.

(6) Use and release of contractor attributional/proprietary information created by or for DoD. Information that is obtained from the contractor (or derived from information obtained from the contractor) under this part that is created by or for DoD (including the information submitted pursuant to paragraph (b) of this section) is authorized to be used and released outside of DoD for purposes and activities authorized by this section, and for any other lawful Government purpose or activity, subject to all applicable statutory, regulatory, and policy based restrictions on the Government's use and release of such information.

(n) Contractors shall conduct their respective activities under this part in accordance with applicable laws and regulations on the interception, monitoring, access, use, and disclosure of electronic communications and data.

(o) *Freedom of Information Act (FOIA).* Agency records, which may include qualifying information received from non-federal entities, are subject to request under the Freedom of Information Act (5 U.S.C. 552) (FOIA), which is implemented in the DoD by DoD Directive 5400.07 and DoD Regulation 5400.7-R (see 32 CFR parts 285 and 286, respectively). Pursuant to established procedures and applicable regulations, the Government will protect sensitive nonpublic information reported under mandatory reporting requirements against unauthorized public disclosure by asserting applicable FOIA exemptions. The Government will inform the non-Government source or submitter (e.g., contractor or DIB participant of any such information that may be subject to release in response to a FOIA request), in order to permit the source or submitter to support the withholding of such information or pursue any other available legal remedies.

(p) *Other reporting requirements.* Cyber incident reporting required by this part in no way abrogates the contractor's responsibility for other cyber incident reporting pertaining to its unclassified information systems under other clauses that may apply to its contract(s), or as a result of other applicable U.S. Government statutory or regulatory requirements, including Federal or DoD requirements for Controlled Unclassified Information as established by Executive Order 13556, as well as regulations and guidance established pursuant thereto.

§236.5 DoD-DIB CS information sharing program.

(a) All contractors that are CDCs and meet the requirements set forth in § 236.7 are eligible to join the voluntary DoD-DIB CS information sharing program as a DIB participant.

(b) Under the voluntary activities of the DoD-DIB CS information sharing program, the Government and each DIB participant will execute a standardized agreement, referred to as a Framework Agreement (FA) to share, in a timely and secure manner, on a recurring basis, and to the greatest extent possible, cybersecurity information.

(c) Each such FA between the Government and a DIB participant must comply with and implement the requirements of this part, and will include additional terms and conditions as necessary to effectively implement the voluntary information sharing activities described in this part with individual DIB participants.

(d) The DoD-DIB CS Activities Office is the overall point of contact for the program. The DC3 managed DoD-DIB Collaborative Information Sharing Environment (DCISE) is the operational focal point for cyber threat information sharing and incident reporting under the DoD-DIB CS information sharing program.

(e) The Government will maintain a website or other internet-based capability to provide potential DIB participants with information about eligibility and participation in the program, to enable online application or registration for participation, and to support the execution of necessary agreements with the Government.

(f) *GFI.* The Government shall share GFI with DIB participants or designated SP in accordance with this part.

(g) Prior to receiving GFI from the Government, each DIB participant shall provide the requisite points of contact information, to include security clearance and citizenship information, for the designated personnel within their company (e.g., typically 3-10 company designated points of contact) in order to facilitate the DoD-DIB interaction in the DoD-DIB CS information sharing

program. The Government will confirm the accuracy of the information provided as a condition of that point of contact being authorized to act on behalf of the DIB participant for this program.

(h) GFI will be issued via both unclassified and classified means. DIB participant handling and safeguarding of classified information shall be in compliance with DoD 5220.22-M, "National Industrial Security Program Operating Manual (NISPOM)," available at http://www.dss.mil/documents/odaa/nispom2006-5220.pdf. The Government shall specify transmission and distribution procedures for all GFI, and shall inform DIB participants of any revisions to previously specified transmission or procedures.

(i) Except as authorized in this part or in writing by the Government, DIB participants may:

(1) Use GFI only on U.S. based covered contractor information systems, or U.S. based networks or information systems used to provide operationally critical support; and

(2) Share GFI only within their company or organization, on a need-to-know basis, with distribution restricted to U.S. citizens.

(j) In individual cases DIB participants may request, and the Government may authorize, disclosure and use of GFI under applicable terms and conditions when the DIB participant can demonstrate that appropriate information handling and protection mechanisms are in place and has determined that it requires the ability:

(1) To share the GFI with a non-U.S. citizen; or

(2) To use the GFI on a non-U.S. based covered contractor information system; or

(3) To use the GFI on a non-U.S. based network or information system in order to better protect a contractor's ability to provide operationally critical support.

(k) DIB participants shall maintain the capability to electronically disseminate GFI within the Company in an encrypted fashion (e.g., using Secure/Multipurpose Internet Mail Extensions

(S/MIME), secure socket layer (SSL), Transport Layer Security (TLS) protocol version 1.2, DoD-approved medium assurance certificates).

(l) DIB participants shall not share GFI outside of their company or organization, regardless of personnel clearance level, except as authorized in this part or otherwise authorized in writing by the Government.

(m) If the DIB participant utilizes a SP for information system security services, the DIB participant may share GFI with that SP under the following conditions and as authorized in writing by the Government:

(1) The DIB participant must identify the SP to the Government and request permission to share or disclose any GFI with that SP (which may include a request that the Government share information directly with the SP on behalf of the DIB participant) solely for the authorized purposes of this program.

(2) The SP must provide the Government with sufficient information to enable the Government to determine whether the SP is eligible to receive such information, and possesses the capability to provide appropriate protections for the GFI.

(3) Upon approval by the Government, the SP must enter into a legally binding agreement with the DIB participant (and also an appropriate agreement with the Government in any case in which the SP will receive or share information directly with the Government on behalf of the DIB participant) under which the SP is subject to all applicable requirements of this part and of any supplemental terms and conditions in the DIB participant's FA with the Government, and which authorizes the SP to use the GFI only as authorized by the Government.

(n) The DIB participant may not sell, lease, license, or otherwise incorporate the GFI into its products or services, except that this does not prohibit a DIB participant from being appropriately designated an SP in accordance with paragraph (m) of this section.

§236.6 General provisions of the DoD-DIB CS information sharing program.

(a) Confidentiality of information that is exchanged under the DoD-DIB CS information sharing program will be protected to the maximum extent authorized by law, regulation, and policy. DoD and DIB participants each bear responsibility for their own actions under the voluntary DoD-DIB CS information sharing program.

(b) All DIB CS participants may participate in the Department of Homeland Security's Enhanced Cybersecurity Services (ECS) program (http://www.dhs.gov/enhanced-cybersecurity-services).

(c) Participation in the voluntary DoD-DIB CS information sharing program does not obligate the DIB participant to utilize the GFI in, or otherwise to implement any changes to, its information systems. Any action taken by the DIB participant based on the GFI or other participation in this program is taken on the DIB participant's own volition and at its own risk and expense.

(d) A DIB participant's participation in the voluntary DoD-DIB CS information sharing program is not intended to create any unfair competitive advantage or disadvantage in DoD source selections or competitions, or to provide any other form of unfair preferential treatment, and shall not in any way be represented or interpreted as a Government endorsement or approval of the DIB participant, its information systems, or its products or services.

(e) The DIB participant and the Government may each unilaterally limit or discontinue participation in the voluntary DoD-DIB CS information sharing program at any time.

Termination shall not relieve the DIB participant or the Government from obligations to continue to protect against the unauthorized use or disclosure of GFI, attribution information, contractor proprietary information, third-party proprietary information, or any other information exchanged under this program, as required by law, regulation, contract, or the FA.

(f) Upon termination of the FA, and/or change of Facility Security Clearance (FCL) status below Secret, GFI must be returned to the Government or destroyed pursuant to direction of, and at the discretion of, the Government.

(g) Participation in these activities does not abrogate the Government's, or the DIB participants' rights or obligations regarding the handling, safeguarding, sharing, or reporting of information, or regarding any physical, personnel, or other security requirements, as required by law, regulation, policy, or a valid legal contractual obligation. However, participation in the voluntary activities of the DoD-DIB CS information sharing program does not eliminate the requirement for DIB participants to report cyber incidents in accordance with § 236.4.

§236.7 DoD-DIB CS information sharing program requirements.

(a) To participate in the DoD-DIB CS information sharing program, a contractor must be a CDC and shall:

(1) Have an existing active FCL granted under the NISPOM (DoD 5220.22-M); and

(2) Execute the standardized FA with the Government (available during the application process), which implements the requirements set forth in §§ 236.5 through 236.7, and allows the CDC to select their level of participation in the voluntary DoD-DIB CS information sharing program.

(3) In order for participating CDCs to receive classified cyber threat information electronically, they must:

(i) Have or acquire a Communication Security (COMSEC) account in accordance with the NISPOM Chapter 9, Section 4 (DoD 5220.22-M), which provides procedures and requirements for COMSEC activities; and

(ii) Have or acquire approved safeguarding for at least Secret information, and continue to qualify under the NISPOM for retention of its FCL and approved safeguarding; and

(iii) Obtain access to DoD's secure voice and data transmission systems supporting the voluntary DoD-DIB CS information sharing program.

(b) [Reserved]

Dated: September 14, 2015.

Patricia L. Toppings,
OSD Federal Register
Liaison Officer,
Department of Defense.
[FR Doc. 2015-24296 Filed: 10/1/2015 08:45 am; Publication Date: 10/2/2015]