Department of Defense assumes no responsibility for the payment of any fees or costs related to such removal which may be charged to the owner of the vehicle by the towing organization. This section may be supplemented from time to time with the approval of the Director, Washington Headquarters Services, or his designee, or the Installation Commander, by the issuance and posting of such parking directives as may be required, and when so issued and posted such directive shall have the same force and effect as if made a part hereof.

§ 234.19 Penalties and effect on other laws.

(a) Whoever shall be found guilty of willfully violating any rule or regulation enumerated in this part is subject to the penalties imposed by Federal law for the commission of a Class B misdemeanor offense.

(b) Whoever violates any rule or regulation enumerated in this part is liable to the United States for a civil penalty of not more than $1,000.

(c) Nothing in this part shall be construed to abrogate any other Federal laws.

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

Sec.

AUTHORITY: 10 U.S.C. 391, 393, and 2224; 44 U.S.C. 3506 and 3554; 50 U.S.C. 3330.

SOURCE: 80 FR 59584, Oct. 2, 2015, unless otherwise noted.

§ 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 permits eligible DoD contractors to participate in the voluntary DIB CS Program to share cyber threat information and cybersecurity best practices with DIB CS Program participants. The DIB CS Program enhances and supplements DIB CS Program participants' capabilities to safeguard DoD information that resides on, or transits, DIB unclassified information systems.

[80 FR 59584, Oct. 2, 2015, as amended at 81 FR 68317, Oct. 4, 2016; 89 FR 17747, Mar. 12, 2024]

§ 236.2 Definitions.

As used in this part:

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

(1) Marked or otherwise identified in an agreement and provided to the contractor by or on behalf of the DoD in support of the performance of the agreement; or

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

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 CS Program participant means a contractor that has met all of the eligibility requirements to participate in the voluntary DIB CS 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 DIB CS 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.

[80 FR 59584, Oct. 2, 2015, as amended at 81 FR 68317, Oct. 4, 2016; 89 FR 17747, Mar. 12, 2024]

EDITORIAL NOTE: At 81 FR 68317, Oct. 4, 2016, § 236.2 was amended; however, a portion of the amendment could not be incorporated due to inaccurate amendatory instruction.

§ 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 CS Program participants 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 DIB CS Program.

[80 FR 59584, Oct. 2, 2015, as amended at 81 FR 68317, Oct. 4, 2016; 89 FR 17747, Mar. 12, 2024]

§ 236.4 Mandatory cyber incident reporting procedures.

(a) *Applicability and order of precedence.* The requirement to report cyber incidents shall be included in all forms of agreements (*e.g.*, contracts, grants, cooperative agreements, other transaction agreements, technology investment agreements, and any other type of legal instrument or agreement) 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 *https://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 *https://dibnet.dod.mil.*

(d) *Subcontractor reporting procedures.* Contractors shall flow down the cyber incident reporting requirements of this part to their subcontractors that are providing operationally critical support or for which subcontract performance will involve a covered contractor information system. Contractors shall require subcontractors to rapidly report cyber incidents directly to DoD at *https://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) *Procurement Integrated Enterprise Environment (PIEE) account requirement.* To report cyber incidents in accordance with this section, the contractor or subcontractor shall have a PIEE account to access *https://dibnet.dod.mil.* For information on obtaining a PIEE account, see *https://piee.eb.mil/.*

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

(g) *Voluntary information sharing.* 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 (i) 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 non-attributional cyber threat information with defense 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.

(n) 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.

(o) *Contractor activities.* 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.

(p) *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). The Government will notify the non-Government source or submitter (*e.g.*, contractor or DIB CS Program participant) of the information in accordance with the procedures in 32 CFR 286.10.

(q) *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.

[80 FR 59584, Oct. 2, 2015, as amended at 81 FR 68317, Oct. 4, 2016; 89 FR 17747, Mar. 12, 2024]

§ 236.5 DoD's DIB CS Program.

(a) All defense contractors that meet the requirements set forth in § 236.7 are eligible to join the DIB CS Program as a DIB CS Program participant. Defense contractors meeting the additional eligibility requirements in § 236.7 can elect to access and receive classified information electronically.

(b) Under the voluntary activities of the DIB CS Program, the Government and each DIB CS Program 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 CS Program 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 CS Program participants.

(d) DoD's DIB CS Program Management 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 DIB CS Program.

(e) The Government will maintain a website or other internet-based capability to provide potential DIB CS Program 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) As participants of the DIB CS Program, defense contractors are encouraged to share cyber threat indicators and information that they believe are valuable in alerting the Government and other DIB CS Program participants to better counter threat actor activity. Cyber activity that is not covered under § 236.4 may be of interest to DIB CS Program participants and DoD.

(g) The Government shall share GFI DIB CS Program participant or designated SP in accordance with this part.

(h) Prior to receiving GFI, each DIB CS Program participant shall provide the requisite points of contact information, to include U.S. citizenship and security clearance information, as applicable, for the designated personnel within their company in order to facilitate the DoD–DIB interaction in the DIB CS 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 CS Program participant for this program.

(i) GFI will be issued via both unclassified and classified means. DIB CS Program participants handling and safeguarding of classified information shall be in compliance with 32 CFR part 117. The Government shall specify transmission and distribution procedures for all GFI, and shall inform DIB CS Program participants of any revisions to previously specified transmission or procedures.

(j) Except as authorized in this part or in writing by the Government, DIB CS Program 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.

(k) In individual cases DIB CS Program participants may request, and the Government may authorize, disclosure and use of GFI under applicable terms and conditions when the DIB CS Program 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.

(l) DIB CS Program 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).

(m) DIB CS Program 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.

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

(1) The DIB CS Program 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 CS Program 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 CS Program 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 CS Program participant) under which the SP is subject to all applicable requirements of this part and of any supplemental terms and conditions in the DIB CS Program participant's FA with the Government, and which authorizes the SP to use the GFI only as authorized by the Government.

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

[80 FR 59584, Oct. 2, 2015, as amended at 81 FR 68317, Oct. 4, 2016; 89 FR 17747, Mar. 12, 2024]

§ 236.6 General provisions of DoD's DIB CS Program.

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

(b) All DIB CS Program participants may participate in the Department of Homeland Security's Enhanced Cybersecurity Services (ECS) program (*https://www.cisa.gov/resources-tools/programs/enhanced-cybersecurity-services-ecs*).

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

(d) A DIB CS Program participant's participation in the voluntary DIB CS 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 CS Program participant, its information systems, or its products or services.

(e) The DIB CS Program participant and the Government may each unilaterally limit or discontinue participation in the voluntary DIB CS Program at any time. Termination shall not relieve the DIB CS Program 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, change of status as a defense contractor, 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 CS Program 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 DIB CS Program does not eliminate the requirement for DIB CS Program participants to report cyber incidents in accordance with § 236.4.

[80 FR 59584, Oct. 2, 2015, as amended at 81 FR 68317, Oct. 4, 2016; 89 FR 17748, Mar. 12, 2024]

§ 236.7 DoD's DIB CS Program requirements.

(a) To participate in the DIB CS Program, a contractor must own or operate a covered contractor information system and shall execute the standardized FA with the Government (available during the application process), which implements the requirements set forth in §§ 236.5 and 236.6.

(b) In order for DIB CS Program participants to receive classified cyber threat information electronically, the company must be a cleared defense contractor and must:

(1) Have an existing active facility clearance level (FCL) to at least the Secret level in accordance with 32 CFR part 117;

(2) Have or acquire a Communication Security (COMSEC) account in accordance with 32 CFR part 117, which provides procedures and requirements for COMSEC activities;

(3) Have or acquire approved safeguarding for at least Secret information, and continue to qualify under 32 CFR part 117 for retention of its FCL and approved safeguarding; and

(4) Obtain access to DoD's secure voice and data transmission systems supporting the voluntary DIB CS Program.

[89 FR 17749, Mar. 12, 2024]

PART 238—DoD ASSISTANCE TO NON-GOVERNMENT, ENTERTAINMENT-ORIENTED MEDIA PRODUCTIONS

Sec.

AUTHORITY: 10 U.S.C. 2264; 31 U.S.C. 9701.

SOURCE: 80 FR 47836, Aug. 10, 2015, unless otherwise noted.

§ 238.1 Purpose.

This part establishes policy, assigns responsibilities, and prescribes procedures for DoD assistance to non-Government entertainment media productions such as feature motion pictures, episodic television programs, documentaries, and electronic games.

§ 238.2 Applicability.

This part:

(a) Applies to the Office of the Secretary of Defense, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the combatant commands, the