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 nondisclosure 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 Web site 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