Department of Defense Expands Defense Industrial Base Voluntary Cybersecurity Information Sharing Activities

The Department of Defense (DOD) has expanded its voluntary cybersecurity information sharing activities to all eligible Defense Industrial Base (DIB) companies. Following a pilot program involving a limited number of DIB contractors, DOD is expanding participation in its Voluntary DIB Cyber Security / Information Assurance (CS/IA) Program, including the optional DIB Enhanced Cybersecurity Services (DECS) component. Deputy Secretary of Defense Ashton B. Carter describes the program as “an important step forward in our ability to catch up with widespread cyber threats.”

The program expansion is spelled out in an interim final rule setting forth new regulations that “provide a voluntary framework for DOD and DIB companies to share information to address sophisticated cyber threats that represent an imminent threat to US national security and economic security interests.”

DIB CS/IA Program

Recognizing that critical defense information resides on DIB networks and systems, and cyber threats to DIB unclassified information systems “pose an imminent threat to US national security and economic security interests,” the DIB CS/IA program is designed to enhance DIB participants’ ability to defend against cyber intrusions onto their networks through voluntary information sharing between the government and DIB companies. Under the program, DOD provides cyber threat information and information assurance best practices to the DIB companies to help protect systems that process or store defense information. Participating DIB companies report cyber intrusions affecting their systems, permitting DOD to analyze cyber threats and vulnerabilities, and develop improved response measures.

2 Id.
4 Id. at 27615, 32 C.F.R. § 236.1.
DECS
The DECS is a joint activity between DOD and the Department of Homeland Security (DHS), within DHS’ Joint Cybersecurity Services Program. Under the DECS component, the government furnishes classified threat and technical information, including known malicious code signatures, to participating DIB companies, or their Internet service providers, which enables them to counter these known cyber threats by scanning the participating DIB companies’ Internet traffic. DHS is the point of contact for participating Internet service providers, and Internet service providers capable of using the government-furnished information to counter the cyber threats in compliance with applicable security requirements are eligible to offer cybersecurity services to DIB participants through the DECS program. Once a company is participating in the DIB CS/IA Program, it can elect to participate in DECS by meeting the security requirements to implement countermeasures on its own networks or by purchasing the services from a participating Internet service provider.

Regulatory Framework (32 C.F.R. Part 236)
The interim final rule establishes new part 236 in title 32 of the Code of Federal Regulations to govern information sharing under the DIB CS/IA program. DOD is accepting comments until July 10, 2012, and the final regulations may be modified.

Eligibility
The DIB includes the DOD, United States government, and the “private sector worldwide industrial complex with capabilities to perform research and development, design, produce, and maintain military weapons systems, subsystems, components, or parts to satisfy military requirements.” A DIB company is eligible to participate in the expanded DIB CS/IA program, if it has a Facility Security Clearance (FCL) for at least Secret information.

Each DIB participant must execute with the government a voluntary, standardized agreement, known as a Framework Agreement (FA), implementing the requirements of the DIB CS/IA program and memorializing the responsibilities of the DIB participant and the government under the program. The DOD has established a public website for the DIB CS/IA Program (http://dibnet.dod.mil/) with information and an online application process.

Bilateral Information Sharing
The DIB CS/IA program focuses on safeguarding “covered defense information,” which is defined as seven specific types of sensitive, but unclassified information provided to a DIB participant in connection with an official DOD activity or collected by the DIB participant in support of an official DOD activity: (i) technical information marked for restricted distribution, (ii) information subject to export controls under the International Traffic in Arms Regulations (ITAR) or the Export Administration Regulations (EAR), (iii) Critical Program Information, (iv) Personally Identifiable Information (PII), (v) information bearing designations indicating controlled access (e.g., For Official Use Only), (vi) information that could be useful to hostile intelligence systems, and (vii) other information exempt from public disclosure under the Freedom of Information Act.

Under the program, the government “shall” share with participants, through both unclassified and classified means, government furnished information (GFI), including cyber threat information and information assurance best practices, to defend against cyber threats. Although the new regulation states that the government “shall” provide

7 DOD Fact Sheet: Defense Industrial Base (DIB) Cybersecurity Activities.
8 Id.
9 77 Fed. Reg. 27619, 32 C.F.R. § 236.2(g).
10 Id. at 27621, § 236.7.
11 Id. at 27618, § 236.2(c).
12 Id. at 27620, § 236.5(a).
GFI, the regulation defines GFI as information provided by the government under the voluntary DIB CS/IA program, affording the government discretion to choose what information to share.

In exchange, DIB participants “shall” report cyber incidents involving covered defense information on a covered DIB system to the DOD Cyber Crime Center’s DOD-DIB Collaborative Information Sharing Environment (DC3/DCISE) within 72 hours of discovering an incident, and may also report other cyber incidents relevant to information assurance for defense information and DIB systems. Although the regulations suggest that initial reporting of cyber incidents is mandatory for DIB participants, the regulations further provide that either the DIB participant or the government may unilaterally limit or discontinue participation in the program at any time. After an initial incident report, the government and the DIB participant may voluntarily share additional information regarding the reported intrusion, including forensic analyses, mitigation and remediation strategy, and cyber intrusion damage assessments, and the government may conduct a cyber intrusion damage assessment and share the results of the assessment with DIB participants.

**Handling and Safeguarding of Information**

Recognizing the extremely sensitive nature of the cyber threat information to be exchanged, the regulations require appropriate security measures to safeguard that information from unauthorized disclosure. Generally, DIB participants may use the government-furnished information to protect covered defense information only on covered DIB systems that are U.S.-based, “i.e., provisioned, maintained, or operated within the physical boundaries of the United States,” and must limit distribution of such information to U.S. citizens within the company on a “need to know basis.”

13 Id. § 236.5(b).
14 Id. at 27621, § 236.6(g).
15 Id. at 27620, § 236.5(c) - (d).
16 Id. at 27619, § 236.4.
17 Id. § 236.4(e) - (i).

Classified information must be safeguarded in compliance with the National Industrial Security Program Operating Manual (NISPOM) (DOD 5220.22–M).

To the extent a DIB participant utilizes a third-party service provider for information system security services, the DIB participant must seek approval to share government-furnished information with the service provider, and the service provider must enter into a legally binding agreement imposing upon the service provider the program requirements, as well as any supplemental terms in the DIB participant’s FA with the government.

With regard to information provided by DIB participants, the regulations require the government to take “reasonable steps” to prevent unauthorized release of DIB participants’ attribution and other nonpublic, sensitive or proprietary information, including restricting internal use of participants’ attribution information to only government personnel and support contractors that are bound by appropriate confidentiality and handling restrictions. The government may share non-attribution information with other participants in the DIB CS/IA program and throughout the government for cybersecurity and information assurance purposes to protect government information.

**Interaction with Other Laws, Regulations and Contractual Obligations**

Participation in the DIB CS/IS program is voluntary, and participation does not alter or supersede a DIB participant’s contractual obligations, or other rights or duties regarding the handling or safeguarding of information under other laws or regulations. Activities under the program must be conducted in accordance with “applicable laws and regulations, including restrictions on the interception, monitoring, access, use, and disclosure of electronic communications or data,” and the government and the DIB participant “each bear responsibility for their own actions” under the program.
The new regulations require that, prior to sharing any information with the government under the program, a DIB participant must perform “a legal review of its policies and practices” supporting the company’s participation in the DIB CS/IA program and must “make a determination that such policies, practices, and activities comply with applicable legal requirements.” The government reserves the right to request from any DIB participant information or assurances regarding the DIB participant’s policies or practices.

**Potential Concerns for Government Contractors**

Participation in the voluntary DIB CS/IA program presents at least two potential concerns that may arise from voluntary cyber incident reporting: (1) disclosure of information from cyber incident reporting and (2) DOD use of cyber incident reports against contractors.

**Disclosure of Information From Cyber Incident Reporting**

Submission of cyber incident information could create the risk of liability to third parties for disclosure of their information, or contractors may incur substantial cost trying to obtain permission to disclose such third-party information. To the extent a contractor discloses to the government without permission third-party data protected by a non-disclosure provision, the third party may seek to hold the contractor liable for the unauthorized disclosure.

There is also risk that DOD’s sharing of threat information derived from incident reports with other participants could result in inadvertent disclosure of a contractor’s proprietary data. Although the new rule restricts the government’s use of attribution information, the government may share non-attribution information provided by DIB participants, or derived from information provided by a DIB participant. This could include information about vulnerabilities, incidents, threats, or countermeasures.

**DOD Use of Cyber Incident Reports Against Contractors.**

There is also the risk that negative information in a cyber incident report potentially could harm the contractor who filed the report. While the government agrees to safeguard participants’ sensitive information from unauthorized uses or disclosures, the program’s use restrictions do not limit the government’s ability to conduct law enforcement or counterintelligence activities, or other lawful activities in the interest of national security. Nor does the interim final rule contain a safe harbor provision for cyber incident reporting. For example, information disclosed by a contractor regarding a cyber incident could lead DOD to independently review the contractor’s information security procedures and its compliance with information security clauses in the contract, or trigger an audit or investigation of the reporting company’s DOD contracting activities affected by a reported cyber incident.

Because program participation is voluntary, however, DOD is incentivized to encourage voluntary reporting by refraining from using voluntary reports aggressively for other enforcement purposes. Further, a contractor’s reporting of a cyber breach under the DIB CS/IA program may merely duplicate a contractor’s mandatory disclosure obligations under other statutory, regulatory, or contractual requirements.

A contractor’s participation in the voluntary program also may influence judgments about the vibrancy of a contractor’s information assurance approach in connection with future contract award decisions. The interim final rule provides that a contractor’s participation in the program “is not intended to create any unfair competitive advantage or disadvantage in DOD source selections,” and cannot be viewed as the government’s endorsement of the contractor or its network capabilities. Notwithstanding this limitation, the rule does not preclude a contractor from describing its participation in the program on a voluntary basis.
the program in future bids, or the agency from considering such participation, to the extent a contractor’s participation may be relevant to a competition.

**Conclusion**

Although participation in the voluntary program may carry some risk, contractors derive benefit from receiving the government-furnished cybersecurity information. Further, as the DIB cybersecurity information sharing plan expands from the original thirty-seven participants, contractors may increasingly decide they need to participate or be at a competitive disadvantage. Ultimately, the reporting obligations under the DIB CS/IA program underscore DOD’s determination to protect DOD information held by the DIB and further heighten the importance of cybersecurity compliance. Given the growing cyber threat environment, this cybersecurity information-sharing program, while now voluntary, may become mandatory eventually, in this or some similar form, in the same way “voluntary” disclosure programs in the False Claims Act area became mandatory disclosure obligations under the Federal Acquisition Regulation (FAR).²⁵

DOD’s expanded voluntary DIB cybersecurity information sharing activities is part of the U.S. government’s increasing efforts to combat cyber threats posing risks to U.S. economic and national security interests. Arnold & Porter LLP will be monitoring the landscape for developments as they occur and can be contacted for updates.

²⁵ FAR 52.203-13.

We hope you have found this Advisory useful. If you would like more information or assistance in addressing the issues raised in this Advisory, please feel free to contact:

**Ronald D. Lee**  
+1 202.942.5380  
Ronald.Lee@aporter.com

**Lauren J. Schlanger**  
+1 202.942.6808  
Lauren.Schlanger@aporter.com