**International Law Advisory**

**DoD’s New Defense Industrial Base Cybersecurity Rule Aligns with the August DFARS Cyber Reporting Rule**

October 8, 2015

Authors
Meredith Rathbone, Edward J. Krauland, Guy Soussan

**Overview**

On October 2, the Office of the Chief Information Officer of the US Department of Defense (DoD) issued an interim final rule relating to the Defense Industrial Base (DIB) Cybersecurity Activities program. The rule is effective immediately; comments are due on December 1. A copy of the rule can be found here. This interim rule is further evidence of the attention being paid to contractor and supply chain cybersecurity risks.

The DIB program is a voluntary cybersecurity-related reporting and information sharing regime in which cleared defense contractors (i.e., those having facility clearances for corporate access to classified national security information) are eligible to participate. It is estimated that nearly 1,000 contractors currently participate. The rule sets forth new DIB participant cyber-reporting requirements and establishes new criteria for entry into the program.

**Cyber Reporting**

Many aspects of the rule are not “new news” in that the requirements regarding DIB participant cyber-reporting largely mimic those already included in the DFARS network penetration and cyber reporting rule which was issued in August and which we summarized in our prior alert. That rule required defense contractors and subcontractors to report to DoD within 72 hours of a cyberhacking incident involving “covered defense information” and to maintain certain records of the incidents. The DIB rules requirements, and the categories of information it covers, are essentially the same.

Notably, however, the interim DIB rule states that it relates to contracts, other transactions and grants in which DIB companies participate, so its coverage is greater than the August rule which was only directly relevant to procurement contracting. In addition, although the DIB is a voluntary program, the rule’s reporting requirements would appear to sweep in subcontractors who are not participants, as the rule requires DIB participants to require that their subcontractors report. Therefore, a subcontractor of a DIB participant working under a grant may be obliged to report under the new regime.

Like the DFARS rule, the DIB rule emphasizes the importance of informing DoD of potential hacking incidents involving export controlled information. In that regard, the preamble specifically states that the rule’s reporting requirements are geared in part at ensuring the DoD will be informed of apparent compromises of export controlled information. Like the August DFARS rule, however, the DIB rule does not precisely define export controlled information, which could cause confusion in the defense contracting community, e.g., is low level “EAR 99” technical data covered? As we indicated in our prior alert, the “mandatory” element of reporting to DoD, whether under the DFARS rule or the “voluntary” DIB program, could result in company’s needing to assess whether they should also be self-reporting to relevant export control agencies.
Contractors should note that the mandatory reporting under this interim final rule is not a substitute for any other reporting requirements. The rule expressly notes that “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.” In addition, the rule explicitly states that “reporting under this program does not abrogate the contractor’s responsibility for any other applicable cyber incident reporting requirements, such breaches to classified systems.”

Finally, the rule contains additional information about where to report, how to obtain the credentials to report, and also indicates that third party service providers (SP) that assist contractors with cybersecurity can also report on behalf of those contractors.

**Entry to Program/Program Basics**

The rule also facilitates expanded entry to the DIB program. It notes that all contractors that have facility clearances and meet the requirements of the rule are eligible to join the voluntary DoD-DIB CS information sharing program as a DIB participant.

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.

Each such FA between the US Government and a DIB participant must comply with and implement the requirements of the DIB program regulations, and is required to include additional terms and conditions as necessary to effectively implement the voluntary information sharing activities described in the regulations with individual DIB participants.

Under the program, the US Government shall share Government Furnished Information (GFI) with DIB participants or designated SP in accordance with the regulations. Prior to receiving GFI from the US 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 US 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.

The US Government can issue GFI via both unclassified and classified means. DIB participant handling and safeguarding of classified information is required to be compliance with DoD 5220.22-M, “National Industrial Security Program Operating Manual (NISPOM).” The US Government is required to specify transmission and distribution procedures for all GFI and inform DIB participants of any revisions to previously specified transmission or procedures. Except as authorized in the regulations or in writing by the US Government, the rule notes that DIB participants may:

1. Use GFI only on US based covered contractor information systems, or US 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 US citizens.

In individual cases the rule states that DIB participants may request, and the US 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-US citizen; or
2. To use the GFI on a non-US based covered contractor information system; or
3. To use the GFI on a non-US based network or information system in order to better protect a contractor’s ability to provide operationally critical support.

DIB participants are required to 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).

The rule further notes that 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 US Government.

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 US 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 GFI is not classified 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.” In addition, the rule explicitly states that “reporting under this program does not abrogate the contractor’s responsibility for any other applicable cyber incident reporting requirements, such breaches to classified systems.”
Sp is eligible to receive such information, and possesses the capability to provide appropriate protections for the GFI.

Upon approval by the US Government, the SP must enter into a legally binding agreement with the DIB participant (and also an appropriate agreement with the US Government in any case in which the SP will receive or share information directly with the US 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 US Government, and which authorizes the SP to use the GFI only as authorized by the US Government.

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 the rule.

Practices
 Export Controls
 Government Contracts
 National Security/CFIUS