PAUL HASTINGS

STAY CURRENT

October 2016

Follow @Paul_Hastings

Cyberattack Reporting Rule for Federal Contractors Finalized

By Charles A. Patrizia & Mary-Elizabeth M. Hadley

The U.S. Department of Defense ("DoD") has promulgated a new rule, effective November 3, 2016, that requires federal defense contractors and subcontractors to report within 72 hours any cyber incidents "that result in an actual or potentially adverse effect on a covered contractor information system" (or "covered defense information residing therein"), or that affect "a contractor's ability to provide operationally critical support."[1] Through the rule, DoD seeks to create a single reporting mechanism for contractors' *unclassified* DoD networks or information systems.[2] The rule also establishes eligibility criteria for participation in the DoD's *voluntary* Defense Industrial Base ("DIB") Cyber Security ("CS") Program for sharing cyber threat information and cybersecurity best practices with DIB CS participants.

I. Cyber Incident Reporting Requirement

A. Coverage

The rule's mandatory reporting requirements apply broadly to all forms of agreements between DoD and DIB companies, including contracts, grants, cooperative agreements, technology investment agreements as well as "any other type of legal instrument or agreement."[3] Under § 236.4(d) of the rule, contractors must flow down the reporting requirements to ''subcontractors that are providing operationally critical support or for which subcontract performance will involve a covered contractor information system.''[4] Subcontractors must rapidly report covered cyber incidents directly to DoD as well as to the prime contractor (or next higher-tier subcontractor).[5]

In defining the "covered defense information" subject to the rule, DoD has harmonized the term with the definition of "controlled unclassified information" utilized elsewhere in the Code of Federal Regulations, as well as with provisions of the Defense Federal Acquisition Regulation Supplement ("DFARS") and Federal Acquisition Regulations ("FARs").[6]

Although the rule also defines the term "operationally critical support," the DoD has promised to develop procedures "to ensure that contractors are notified when they are providing supplies or services designated as operationally critical support."[7] For now, contractors are left to report any incident involving "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."[8]

B. 72-Hour Requirement

Covered incidents must be "rapidly" reported "within 72 hours of discovery."[9] In defending the reporting requirement against a commenter's challenge, the DoD explained that "[t]imeliness in reporting cyber incidents is a key element in cybersecurity and provides the clearest understanding of the cyber threat targeting DoD information and the ability of companies to provide operationally critical support."[10]

The DoD further explained that the 72-hour reporting time frame has been part of its DIB CS program since 2008 and, since that time, "has proven to be an effective balance of the need for timely reporting while recognizing the challenges inherent in the initial phases of investigating a cyber incident."[11] Available information should be reported within 72 hours, with updates as needed if additional information becomes available.[12]

Among the information to be included in the initial report are an assessment of the impact of the cyber incident, description of the technique or method used, and a summary of information compromised.[13]

C. Associated Costs

In addition to costs associated with identifying, analyzing, and reporting security incidents and their impact on covered defense information or a contractor's ability to provide operationally critical support, contractors are obligated to obtain "DoD-approved medium assurance certificates to ensure authentication and identification when reporting cyber incidents to DoD."[14] Such certificates, which typically cost approximately $175 each, are "individually issued digital identity credentials used to ensure the identity of the user in online environments."[15]

D. Other Obligations Remain

Contractors remain responsible for complying with any other applicable cyber incident reporting requirements. In reporting incidents involving classified information on classified contractor systems, for example, contractors must comply with the National Industrial Security Program Operating Manual ("NISPOM").[16] With respect to contractors' unclassified networks, however, DoD has noted that it is working to streamline reporting procedures within the Department, including through the designation of the DoD Cyber Crime Center (known as "DC3") as the sole DoD focal point for the receipt of cyber incident reporting.[17]

II. Voluntary Cyber Threat and Cybersecurity Information Sharing

In addition to the mandatory reporting requirements, the rule also addresses voluntary participation in the DIB CS information sharing program—modifying the eligibility criteria to enable greater participation.[18]

A. Benefits of the Program

The DIB CS program offers eligible DIB participants the ability to receive cyber threat information from the government and other DIB contractors, leading to enhanced insight into adversarial activities threatening them.[19] Through the program, participating companies and DoD can exchange "actionable" information that can help "bolster cybersecurity posture."[20] Additionally, the program provides participants with technical assistance from the DoD Cyber Crime Center (DC3), including analyst-to-analyst exchanges, strategies for mitigation and remediation, and guidance on best practices.[21]

B. Participation Requirements

To participate in the DIB CS program under the rule, a contractor must satisfy a number of criteria. First, it must be a cleared defense contractor ("CDC"), defined as "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."[22] Additionally, it must (i) have an existing, active facility clearance ("FCL") to at least the Secret level; (ii) execute a standardized framework agreement ("FA") with the government (which implements the requirements set out in sections 236.5-236.7), and allows the CDC to select its level of participation in the voluntary program; and (iii) to the extent it shall receive classified cyber threat information electronically, comply with additional secure access requirements.[23]

III. Conclusion

Covered contractors and subcontractors should assess their incident response policies and procedures to ensure they have adequate mechanisms in place to identify and report security incidents to the DoD in the required 72 hours. Additionally, if eligible, entities should consider joining the DIB CS program to benefit from the exchange of potential threat information with the government and other contractor participants.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:

Washington, D.C.

Behnam Dayanim
1.202.551.1737
bdayanim@paulhastings.com

Charles A. Patrizia
1.202.551.1710
charlespatrizia@paulhastings.com

Sherrese M. Smith
1.202.551.1965
sherresesmith@paulhastings.com

Mary-Elizabeth M. Hadley
1.202.551.1750
maryelizabethhadley@paulhastings.com

San Francisco

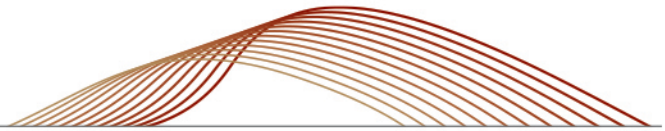
Thomas P. Brown
1.415.856.7248
tombrown@paulhastings.com

Thomas A. Counts
1.415.856.7077
tomcounts@paulhastings.com

Paul M. Schwartz
1.415.856.7090
paulschwartz@paulhastings.com

New York

James H. Koenig
1.212.318.6005
jimkoenig@paulhastings.com



[1] 81 Fed. Reg. 68312.

[2] *Id.*

[3] *Id.*

[4] 32 C.F.R. § 236.4(d).

[5] *Id.*

[6] *See* 32 C.F.R. § 236.2 (defining "covered defense information" as "unclassified controlled technical information or other information (as described in the Controlled Unclassified Information (CUI) Registry … 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"); *see also* 81 Fed. Reg. 68313 (noting that the definition "is also harmonized" with "DFARS Case 2013–D018, ''Network Penetration Reporting and Contracting for Cloud Services" and FAR Case 2011–020, ''Basic Safeguarding of Contractor Information Systems.").

[7] 81 Fed. Reg. 68314.

[8] 32 C.F.R. § 236.2.

[9] *Id.*

[10] 81 Fed. Reg. 68314.

[11] *Id.*

[12] *Id.*

[13] *Id.* at 68315.

[14] *Id.* at 68313.

[15] *Id.*

[16] *Id.* at 68312.

[17] *Id.* at 68314.

[18] *Id.* at 68312.

[19] *Id.*

[20] *Id.* at 68312-68313.

[21] *Id.* at 68313.

[22] 32 C.F.R. § 236.2.

[23] 32 C.F.R. § 236.7(a).