Bloomberg BNA

Privacy and Security Law Report®

A Closer Look at the Department of Defense's Cybersecurity Rule on Adequate Security and 'Cyber Incident' Reporting



BY CHARLES BLANCHARD, RONALD LEE AND NICHOLAS TOWNSEND

Much has been written about the recent Department of Defense (DOD) rule on adequate security and ''cyber incident'' reporting, which was issued Nov. 18, 2013, but several significant implementation issues deserve closer examination.[1]

The final rule imposed two new requirements. First, the rule imposed an obligation on contractors to provide ''adequate security'' to safeguard ''unclassified controlled technical information'' (UCTI).[2] Second, contractors are obligated to report ''cyber incidents'' that affect UCTI to contracting officers.[3] In both obligations, UCTI is defined as ''technical information with military or space application that is subject to controls on access, use, reproduction, modification, performance, display, release, disclosure, or dissemination.''[4] UCTI should be marked with a DOD ''distribution statement.''[5] This is the first time that the DOD has imposed specific requirements for cybersecurity that are generally applicable to all contractors.

These new requirements raise challenging implementation issues for all DOD contractors. As described below, most of these issues are best addressed up-front, including a written incident response plan.

Safeguarding UCTI Issues

The rule imposed a new obligation on contractors to provide ''adequate security to safeguard unclassified controlled technical information'' from ''compromise,'' which is defined as ''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

[1] Defense Federal Acquisition Regulation Supplement: Safeguarding Unclassified Controlled Technical Information (DFARS Case 2011-D039), 78 Fed. Reg. 69,273 (Nov. 18, 2013), *available at* http://www.gpo.gov/fdsys/pkg/FR-2013-11-18/pdf/2013-27313.pdf (12 PVLR 1987, 11/25/13).

Charles Blanchard is a partner in Arnold & Porter LLP's Washington office and is a member of the firm's Government Contracts and National Security practices. Blanchard previously served as general counsel and chief ethics officer for the U.S. Air Force and as general counsel for the U.S. Army.

Ronald Lee is a national security and government contracts partner in Arnold & Porter's Washington office. Lee previously served as general counsel at the National Security Agency.

Nicholas Townsend is an associate in Arnold & Porter LLP's National Security and Public Policy practices in Washington.

[2] *Id.* at 69,280.
[3] *Id.*
[4] *Id.*
[5] DOD, *Instruction No. 5230.24, Distribution Statements on Technical Documents* (Aug. 23, 2012), *available at* http://www.dtic.mil/whs/directives/corres/pdf/523024p.pdf.

 ISSN 1538-3423

an object, or the copying of the information to unauthorized media may have occurred.''[6]

This raises several significant implementation issues for contractors:

Is the contractor in possession of UCTI? The rule applies only to UCTI and imposes safeguarding and reporting requirements on UCTI. Thus, the first implementation question that arises is developing processes and systems that put the contractor on notice that it has possession of UCTI, where that information resides and therefore how the safeguarding and ''cyber incident'' reporting obligations apply to the contractor.

What must the contractor do to ensure ''adequate security''? The rule defines ''adequate security'' in very vague terms: ''protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information.''[7] Notably, this is a predictive and harm-based standard, but contractors or subcontractors won't always be in a position to make accurate assessments of the extent of harm to the DOD of loss or compromise of particular UCTI and thus may have difficulty determining what level of security is ''commensurate.''

In order to provide ''adequate security,'' the contractor must implement information systems security in ''its project, enterprise, or company-wide unclassified information technology system(s) that may have unclassified controlled technical information resident on or transiting through them.''[8] The ''may have'' language in this standard might be read to require implementation of such information systems security on an IT system that doesn't currently have UCTI if there is the possibility that the system might have UCTI in the future.

At a minimum, the rule states that adequate security requires implementation of specified National Institute of Standards and Technology (NIST) Special Publication (SP) 80-53 security controls.[9] But implementation of the NIST controls won't necessarily constitute adequate security. Other security measures will be required if a contractor ''reasonably determines that [additional] information systems security measures . . . may be required to provide adequate security in a dynamic environment based on an assessed risk or vulnerability.''[10]

So what is a contractor to do in response to this rather vague requirement?

- At a minimum, all contractors need to ensure full implementation of the NIST special controls. Since these controls closely parallel the ISO 27002 standard,[11] most large defense contractors are likely already using these controls. The challenge will be for smaller contractors to make sure that both they and their subcontractors are using the NIST controls.
- However, the NIST controls aren't a safe harbor. Contractors should have in place a means of identifying any new threats and adopting any additional security measures that might be necessary. As the DOD explained in response to comments, ''In cases where the contractor has information (either obtained from DoD or any other source) that would suggest additional security is required to adequately protect technical information, they must take action to establish that additional security.''[12] Meeting this requirement requires a process to ensure that the contractor has addressed any new threats that are brought to the attention of its employees.

What does the rule mean for use of cloud computing or other third-party vendors? Many contractors are moving many of their IT functions to cloud computing. How will this new rule apply to cloud computing or other outsourced IT solutions? Under the rule, any IT solutions vendor, including a cloud service provider or even an Internet service provider, would be a subcontractor. The contractors will be responsible for ensuring that these service providers comply with the requirements of the rule, in part by exercising significant due diligence about the use of security controls by the cloud service provider, ISP or other outsourced IT solutions vendor.

What controls must be placed on employees? The rule applies to any IT systems on which UCTI is maintained or transited. This means contractors need to carefully assess whether the adequate security standard, including the NIST controls (or equivalent controls), can be applied to all such systems, including home computers, portable computers and mobile devices. Given the challenges of ensuring the required standards are met on employees' home computers, some large contractors already prohibit the use of home equipment for work projects. All contractors would be prudent to carefully examine the use of personal computers, tablets, phones and other mobile devices for contractor business.

Data Breach Reporting Requirement Issues

Under the new ''cyber incident'' reporting requirement, all DOD contractors and subcontractors who have UCTI on their IT system, or who have UCTI that is merely transiting through their systems, must file a report with the DOD within 72 hours of any ''cyber incident.'' A ''cyber incident'' is defined as ''actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein.''[13] Contractors are required to impose the substance of the reporting requirement on their subcontractors.

Here are some issues this requirement raises for contractors:

What is a reportable ''cyber incident''?

[6] Defense Federal Acquisition Regulation Supplement: Safeguarding Unclassified Controlled Technical Information, 78 Fed. Reg. at 69,280.

[7] *Id.*

[8] *Id.*

[9] *Id.*; *see also* NIST, *Security and Privacy Controls for Federal Information Systems and Organizations* (SP 800–53) (Jan. 15, 2014), *available at* http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

[10] Defense Federal Acquisition Regulation Supplement: Safeguarding Unclassified Controlled Technical Information, 78 Fed. Reg. at 69,280.

[11] *See Introduction to ISO 27002 (ISO27002)*, Internal Organization for Standardization, http://www.27000.org/iso-27002.htm (last visited Mar. 11, 2014).

[12] Defense Federal Acquisition Regulation Supplement: Safeguarding Unclassified Controlled Technical Information, 78 Fed. Reg. at 69,275.

[13] *Id.* at 69,280.

  PVLR ISSN 1538-3423

The challenge is that the definition of ''cyber incident'' doesn't include any materiality standard. Fortunately, the regulation doesn't require that all such incidents be reported. Instead, a ''cyber incident'' is only required to be reported if:

- action was taken through the use of computer networks;
- the action resulted in an actual or potentially adverse effect on an information system or the information on that system; and
- the action had one of the following results:
  - possible exfiltration, manipulation or other loss or compromise of UCTI; or
  - the allowance of unauthorized access to an IT system on which UCTI is resident or transits.[14]

The critical requirement here is that the UCTI itself must have been endangered—either through potential compromise or unauthorized access to an IT system on which UCTI is resident or transits. Thus, a denial of service attack that adversely affects an IT system wouldn't be a reportable ''cyber incident'' because UCTI information wasn't endangered. Similarly, constant probes that don't result in any access to UCTI also aren't reportable.

Still, this is an expansive reporting requirement. For example:

- An employee's unauthorized downloading of UCTI onto a flash drive would be reportable because computer networks were used and UCTI was compromised.
- Even absent certainty of actual compromise, the mere existence of malware on an IT system that even potentially gave unauthorized access to UCTI would be reportable.
- Even if there is no evidence that any UCTI was compromised, the discovery of malware that enabled possible infiltration, manipulation or other loss or compromise of UCTI or gave unauthorized access to the IT system on which UCTI is maintained would be reportable.

The bottom line is that the ''cyber incident'' reporting requirement is broad, and contractors must have systems in place that will both capture potential cybersecurity events and evaluate the need for disclosure. Fortunately, because the focus remains on access to UCTI, one possible strategy to limit needed reports is to segregate UCTI on separate IT systems. However, such segregation may be costly and challenging, particularly for companies that are mainly engaged in commercial business and only have a small amount of DOD business. Even if the contractor's IT systems containing UCTI are linked with the contractor's other systems, compromises of the other IT systems wouldn't be reportable provided that controls on the UCTI system prevented such compromises from causing reportable ''cyber incidents'' under the DOD rule. In any event, prudent contractors will already have a data breach response plan that includes a process for evaluating required disclosures.

[14] *Id.* at 69,282.

Other than reporting the incident to the DOD, what actions must contractors take in response to a ''cyber incident''? Contractors must respond to all reported ''cyber incidents'' by:

- reviewing unclassified networks for evidence of compromise;
- reviewing data accessed during the ''cyber incident'' to identify specific UCTI associated with DOD programs, systems or contracts; and
- preserving and protecting images of known affected information systems and all relevant monitoring/packet capture data for at least 90 days.[15]

How does the contractor address proprietary information on its network? The ''cyber incident'' reporting requirement provides that the DOD has the right to conduct its own damage assessment, which includes the right to require the contractor to provide all damage assessment information gathered by the contractor in connection with the post-incident review and preservation requirements discussed above. The contractor must comply with all damage assessment information requests from the DOD for existing files and images, ''unless there are legal restrictions that limit a company's ability to share digital media.'' [16]

This requirement might potentially put a contractor in the uncomfortable position of declining to provide full access to the requested information because of third-party proprietary information concerns. Indeed, contracting officers may be skeptical of claims that access can be denied because of third-party trade secret claims. A disagreement between the contracting officer and the contractor about whether the contractor's legal obligations preclude it from turning information over to the government might potentially result in termination of the contract for default or negative assessment of the contractor's past performance in the Contractor Performance Assessment Reporting System (CPARS).

In response to this dilemma, a prudent contractor should take the following steps:

- As part of its incident response plan, a contractor should include an inventory of any digital media on the IT system that cannot be disclosed to the DOD because of legal restrictions.
- Where possible, a contractor should negotiate the terms of limited and protected release of this data to the DOD in response to a request under this regulation.

Conclusion

The new adequate safeguard and ''cyber incident'' reporting requirements present significant implementation challenges to DOD contractors. With some advance planning contained in a written incident response plan, however, a prudent contractor can address many of these issues before any ''cyber incident'' or data breach. Other issues can be addressed through careful negotiations with the DOD following the disclosure of a ''cyber incident'' to the DOD.

[15] *Id.*
[16] *Id.*