SQUIRE SANDERS

CYBERSECURITY UPDATE

The beginning of 2014 has seen a number of developments in the US regulatory arena relating to cybersecurity, data protection and privacy. In addition, the massive and widely publicized Target Corporation data breach brought cybersecurity risk and the potential damages to the attention of businesses and individuals worldwide, with some estimates of the cost of that breach approaching US$700 million.

While Europe's regulatory regime has focused on cybersecurity primarily from an individual privacy protection perspective, the trend among US government agencies is a focus on overall cyber security standards, protection of critical infrastructure, and protection of not only individual personal information, but also of technical data and defense and critical industry sectors.

DOD Final Rule: Safeguarding Unclassified Controlled Technical Information

The US Department of Defense (DOD) launched the first regulatory volley in late November 2013, with the issuance of final regulations under the Defense Federal Acquisition Regulation Supplement (DFARS), "Safeguarding Unclassified Controlled Technical Information" (DFARS Case 2011–D039). This final rule addition to the DFARS (i) requires private businesses that are DOD contractors to implement adequate security measures to safeguard "unclassified controlled technical information" within contractor information systems from unauthorized access and disclosure, and (ii) prescribes mandatory reporting to DOD with regard to certain cyber intrusion events that affect "unclassified controlled technical information" resident on or transiting through contractor unclassified information systems. The new rule applies not only to businesses that directly contract with DOD, but also to any subcontractors (at any tier) who handle or possess "unclassified controlled technical information," including, as specifically mentioned in the preamble to the rule, subcontractors such as cloud storage providers who provide data hosting for this information.

What type data or information is covered?

The rule clarifies that unclassified controlled technical information is "technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination." Technical information is technical data or computer software, and includes research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code. Controlled technical information is required to be identified in accordance with DOD Instruction 5230.24, "Distribution Statements on Technical Documents." The term does not include information that is lawfully publicly available without restrictions.

The first step any business that handles technical information should take is to assess the extent, if any, to which the business handles or possesses "unclassified controlled technical information" either for its own business purposes, or as part of services provided to other businesses.

What Are the Legal Obligations Under the Rule For a Business That Handles or Possesses Unclassified Controlled Technical Information?

(1) The Adequate Security Requirement - The first requirement for a business subject to the rule is the obligation to **"provide adequate security to safeguard unclassified controlled technical information on their unclassified information systems from unauthorized access and disclosure."** The rule does not define "adequate security," but rather simply declares that "adequate security" means "protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information." The rule does, however, set forth minimum standards that must be met, including:

- Implementation of 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;
- Adherence to applicable (as set forth in the rule) National Institute of Standards and Technology (NIST) Special Publication (SP) 800–53 security controls, or, if these standards are not implemented, the business must justify this failure to the agency and explain how the other or alternative controls achieve equivalent protection; and
- Application of such additional information systems security requirements that the business reasonably determines may be required to provide adequate security in a dynamic environment based on an assessed risk or vulnerability.

In addition to the specific standards set forth in the rule, businesses should consider using the recently issued "NIST Cybersecurity Framework" as a guide to assessing their information system security and justification and documentation of implementation of "adequate security."

(2) The 72 Hour Reporting Requirement – The second requirement of the DFARS rule is a requirement that any business that believes it may have suffered a "reportable cyber incident" **report as much of certain specified information as can be obtained within 72 hours of the incident.** The report must be made via http://dibnet.dod.mil.

The rule broadly defines a "reportable cyber incident" as both (i) a cyber incident involving possible exfiltration, manipulation or other loss or compromise of any unclassified controlled technical information resident on or transiting through the contractor's, or its subcontractors', unclassified information systems, and (ii) any other incident that involves unauthorized access to the contractor's unclassified information system on which unclassified controlled technical information is resident on or transiting.

The specified information that the rule requests be reported includes:

- Data Universal Numbering System (DUNS);
- Contract numbers affected unless all contracts by the company are affected;
- Facility CAGE code if the location of the event is different than the prime Contractor location;
- Point of contact if different than the POC recorded in the System for Award Management (address, position, telephone, email);
- Contracting Officer point of contact (address, position, telephone, email);
- Contract clearance level;
- Name of subcontractor and CAGE code if this was an incident on a subcontractor network;
- DOD programs, platforms or systems involved.
- Location(s) of compromise.
- Date incident discovered;
- Type of compromise (e.g., unauthorized access, inadvertent release, other);
- Description of technical information compromised; and
- Any additional information relevant to the information compromise.

It is important to note that by specifying that the business report "as much of the [specified] information as can be obtained" the rule places great emphasis on the timely reporting of the incident than the completeness of the information, recognizing that a 72 hour time frame may not be sufficient for a business to fully develop the specified information.

The rule stipulates that it does not in any manner waive or vary any other reporting requirements under contract, regulation or other governmental regulation.

(3) The Follow-on Assessment Support Requirement – A third requirement of the rule is a requirement that after reporting the cyber incident, the business must take certain steps to support the government's damage assessment. These obligations include:

- The obligation for the business to conduct further review of its unclassified network for evidence of compromise resulting from a cyber incident that includes, but is not limited to, identifying compromised computers, servers, specific data and users accounts. This includes a requirement to analyze information systems that were part of the compromise, as well as other information systems on the network that were accessed as a result of the compromise;
- The business must review the data accessed during the cyber incident to identify specific unclassified controlled technical information associated with DOD programs, systems or contracts, including military programs, systems and technology;
- The business must preserve and protect images of known affected information systems and all relevant monitoring/packet capture data for at least 90 days from the cyber incident to allow DOD to request information or decline interest;
- If DOD elects to conduct a damage assessment, the government may require that the business provide all of the above damage assessment information. The requirement to share files and images is subject to a limited exception to the extent that there are other legal restrictions that limit a company's ability to share digital media, but if such an exception is claimed, the business must inform the government of the source, nature and prescription of such limitations and the authority responsible.

(4) The Contractual Flow-thru Requirement – The final requirement under the rule is the requirement that the business must include a requirement for compliance as a mandatory flow-thru clause in all subcontracts for commercial items. Although not explicitly stated in the rule, comments in the regulatory preamble to the adoption of the rule appear to clarify that this flow-thru requirement only applies to those subcontractors who handle or possess the unclassified controlled technical information, a class that includes not only subcontractors involved in the relevant government contract, but also other third party vendors and suppliers who supply or provide services that may give them access to this information – such as various IT service vendors who may provide IT services to the business as a whole and not just pertaining to the relevant government contract.

Other Key Aspects of the Regulation

When publishing the final regulation, the Preamble to the Federal Register notice also clarifies a number of related questions and issues that businesses may have.

- The Preamble confirms that Internet service providers (ISPs) and cloud service providers are considered subcontractors, and that a business must insure that such subcontractors comply with the rule.
- The Preamble confirms that the contract administration office is responsible for assessing compliance, and that the contracting officer for a given contract may, at such official's discretion, require that reviews or audits be conducted to confirm compliance.

- While declining the opportunity to confirm that cost of compliance was an allowable cost under federal Cost Accounting Standards, the Preamble expressly includes a statement that nothing in the regulation make such cost unallowable, and that cost of compliance would thus be evaluated in accordance with provisions of the FAR (FAR 31.201-2) and DFARs (DFAR 231) governing allowable costs. Other commentary in the Preamble indicates that the government expects that in many cases the cost of compliance will be allocated over multiple contracts and thus allowable and chargable to indirect cost pools.
- The Preamble confirms that universities and academic institutions are not exempt from the rule if they handle or deal with unclassified controlled technical information.
- The regulation, as originally proposed, had included not only unclassified controlled technical information as the type of data subject to the rule, but also several other classes of information such as personally identifiable information including HIPPA information. Those other classes of information were removed from the final rule.
- The Preamble indicates that additional guidance for reporting and other procedures will be issued at a future date via supplement to the DFARS Procedures, Guidance, and Information (PGI) at http://www.acq.osd.mil/dpap/dars/ under "Publication Notices, but gave no indication of when such guidance might be issued.
- The rule imposes the reporting requirement on both prime and subcontractors, and the Preamble comments that the prime has an obligation to report when a subcontractor has incurred a reportable cyber incident, even if a subcontractor has also made a report. This means that prime contractors should insure that in addition to the inclusion of the required flow-thru provisions, prime contractors should expressly require that subcontractors notify the prime concurrent with the subcontractor's direct notification to DOD.

Contacts

Robert B. Webb III
Partner
Northern Virginia
+1 703 720 7855
robert.webb@squiresanders.com

Karen R. Harbaugh
Principal
Northern Virginia
+1 703 720 7885
karen.harbaugh@squiresanders.com

Robert E. Gregg
Senior Partner
+1 703 720 7880
robert.gregg@squiresanders.com