Cybersecurity Compliance by Department of Defense Contractors

This column is a follow up to one of the topics covered in the Summer 2017 Technology Corner.[1] One of the topics covered there was new compliance obligations facing all companies that have contracts (directly and indirectly) with the U.S. Department of Defense (DoD). These requirements for DoD contractors have been overshadowed by all of the activity surrounding the implementation of the European Union's General Data Protection Regulation. Unfortunately for some, deadlines have passed and many contractors are at risk.

I need to make a disclaimer here. I do represent a company that provides compliance services for DoD contractors. Were it not for that client, however, these rules may have also been under my radar. The topic of companies being unaware of (or ignoring) the DoD cyber requirements was also raised in discussions earlier this summer at a cyber risk summit hosted by the FBI and Department of Justice. That prompted me to address the topic again.

FARS, DFARS and NIST

While I am sure that the details of last year's article are at the forefront of your memory, let me summarize the part about the DoD. Several requirements were issued in connection with the Federal Acquisition Regulations about basic security controls that all contractors needed to put in place. The DoD also promulgated additional requirements in October 2016 which mandatory cyber incident reporting requirements for DoD contractors and subcontractors. All such entities are subject to information safeguarding and cyber incident reporting requirements. Any defense contractor which processes, stores, or transmits defense information is subject to the rules. As a follow up, the National Institute of Standards and Technology (NIST) established requirements and guidelines in Special Publication (SP) 800-171.

The essence of the obligations is that each DoD contractor has to first be able to document that it has controls in place to protect "controlled unclassified information" (CUI)[2] in nonfederal systems and organizations. Each entity must also have a System Security Plan (SSP) that must "describe the boundary of [a government contractor's] information system; the operational environment for the system; how the security requirements are implemented; and the relationships with or connections to other systems." If requested, government contractors will be required to provide the Government with its SSP and any associated Plans of Action and Milestones (POAM). Federal agencies may consider SSPs and PAMs as critical inputs when deciding to award a contract that requires the processing, storing, or transmitting of CUI on a contractor information system.

To make things easy and clear, the DoD issued a simple two-page document entitled "Safeguarding Covered Defense Information – The Basics."[3] One pertinent part I would like to highlight is the first requirements section. I have added the underlining.

> To safeguard covered defense information contractors/subcontractors *must implement NIST SP800-171*, Protecting CUI in Nonfederal Information Systems and Organizations, as soon as practical, *but not later than Dec 31, 2017*
>
> - For contracts awarded prior to 1 Oct 2017, contractors/subcontractors shall notify DoD CIO within 30 days of contract award of any NIST SP 800-171 security requirements not implemented at the time of contract award.
>
> - If the offeror proposes to vary from NIST SP 800-171, they shall submit to the CO a written explanation of why a security requirement is not applicable OR how an alternative security measure is used to achieve equivalent protection.[4]

DoD also published a detailed presentation entitled "Cyber Security Challenges- Protecting DoD's Unclassified Information"[5] that provided details about implementation of security controls, data breach obligations and incident reporting. As the presentation pointed out, however, there were no strong enforcement mechanisms in place. The contractor's obligation is to "attest" to compliance by signing the contract.

The industry has been aware of the deadline and some were scrambling to meet the end of the year compliance date.[6] The message is not getting to everyone or some, especially small and medium-sized businesses, are waiting for the "knock on the door" before taking action.

Enforcement Moves Forward (Slowly)

It is probably not surprising that the lack of a real enforcement mechanism did not push compliance to the forefront when annual budgets are put into place by companies. Recent activity by the DoD indicates that there is a concern, however. In April, proposed guidance entitled "DoD Guidance for Reviewing System Security Plans and the NIST SP 800-171 Security Requirements Not Yet Implemented" was published in the Federal Register.[7] Also published was a detailed template to guide contractors in the System Security Plan assessment.[8] While the DoD has made it clear that it will not certify compliance, it has indicated that the next steps will be to assess compliance and it is making plans to start that process.

Part of the process started in May 2018 when a memorandum was distributed by the Under Secretary of Defense Kernan that tasked a DoD department with developing a plan for oversight of information data protection across the defense industrial base.[9] The infiltration by Chinese hackers of a Navy contractor that resulted in the theft of classified submarine warfare information[10] will likely accelerate this process.

Conclusions

At some point, each of your clients that have DoD contracts will be asked to prove compliance. The inability to show that will likely result in adverse actions against the client's business, perhaps including debarment. Better safe than sorry is the key take-away here, especially since the date by which compliance was required has long since passed.

Michael S. Khoury is a partner in the Detroit office of FisherBroyles, LLP, and specializes in business, technology transactions, privacy and data security and international law. He is a past Chair of the State Bar of Michigan Business and Information Technology Law Sections.

NOTES

1. Michael S. Khoury, Martin B. Robins, Kimberly Dempsey Booher, and Geoffrey M. Goodale, *Technology Corner: Data Breach and Cyber Incident Response Planning*, MI Bus LJ, Summer 2017, at 8-10.
2. See https://www.archives.gov/cui/registry/category-list.
3. See http://business.defense.gov/Portals/57/Safeguarding%20Covered%20Defense%20Information%20-%20The%20Basics.pdf.
4. *Id.*
5. See https://business.defense.gov/Portals/57/SBTW18%20Cybersecurity%20Update.pdf?ver=2018-04-20-164708-217.
6. http://www.govtech.com/blogs/lohrmann-on-cybersecurity/government-contractors-face-new-year-security-deadline-for-dod.html.
7. https://www.federalregister.gov/documents/2018/04/24/2018-08554/dod-guidance-for-reviewing-system-security-plans-and-the-nist-sp-800-171-security-requirements-not.
8. https://csrc.nist.gov/CSRC/media/Publications/sp/800-171/rev-1/final/documents/CUI-SSP-Template-final.docx.
9. TBD.
10. https://www.washingtonpost.com/world/national-security/china-hacked-a-navy-contractor-and-secured-a-trove-of-highly-sensitive-data-on-submarine-warfare/2018/06/08/6cc396fa-68e6-11e8-bea7-c8eb28bc52b1_story.html?noredirect=on&utm_term=.4ee3605c9c91 and https://www.nytimes.com/2018/06/08/us/politics/china-hack-navy-contractor-.html.