Published by *Aerospace & Defense Law360* on January 27, 2014. Also ran in *Government Contracts Law360*, *Privacy Law360*, *Public Policy Law360* and *Technology Law360.*

2014 Promises To Be Another Banner Year For Cybersecurity

--By Charles Blanchard, Arnold & Porter LLP

Law360, New York (January 27, 2014, 1:22 PM ET) -- While cybersecurity legislation was stalled in Congress, 2013 turned out to be a banner year for cybersecurity regulation, with the U.S. Department of Defense taking the lead with several significant cybersecurity initiatives. The key takeaway of these developments is that the Obama administration is taking full advantage of the leverage they have —particularly over government contractors — to impose mandatory cybersecurity standards on large sectors of the economy. And with the National Institute of Standards and Technology (NIST) posed to issue its final cybersecurity framework on Feb. 13 — a document that will broadly affect all industries — this year also promises to be a banner year.

Last February, after Congress had failed to pass cybersecurity legislation, President Obama issued an executive order and a presidential policy directive that laid out a set of ambitious goals for cybersecurity. Perhaps most critically, in Section 10 of the executive order, all agencies with responsibility for regulating the security of critical infrastructure are ordered to start a process of developing mandatory cybersecurity requirements based on the cybersecurity framework that will be developed by NIST.

While NIST won't issue its framework until the middle of February, the Department of Defense had already been working on cybersecurity regulations to be applied to defense contractors and issued three key regulations that together impose significant new obligations on defense contractor. The new DOD regulations include (1) a requirement to "adequately safeguard" IT systems, (2) a requirement to report cyber incidents, and (3) a new rule on mitigating supply chain risks (such as from malware embedded in components of weapon systems).

In 2014, we can expect that NIST will issue its final cybersecurity framework, that the Federal Acquisition Regulation Council will issue a FAR provision on cybersecurity that may well mirror the DOD rule, and that other agencies will follow the DOD's lead in imposing further cybersecurity regulations on regulated industries.

Looking Back at 2013: DOD Rules on Adequate Security, Cyber Incident Reporting and Supply Side Risk

Last fall was a busy time for DOD efforts to ensure cybersecurity by its contractors. On Nov. 18, 2013, the U.S. Department of Defense issued a final rule that created two new obligations for defense contractors, as well as an interim rule on supply side risk.

The final rule imposed two new requirements. First, the rule imposes an obligation on contractors to provide "adequate security" to safeguard "unclassified technical information" (UCTI). Second, contractors are obligated to report "cyber incidents" that affect UCTI to contracting officers. 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." Both of these new requirements will be incorporated in all new DOD solicitations and contracts.

That same day, the DOD also issued an interim Defense Federal Acquisition Regulation Supplement rule on supply side risk that addressed the risk of malicious embeds introduced in the supply chain for new products.

Safeguarding UCTI

Perhaps the most significant development in the new DOD regulation is a new obligation on contractors to provide "adequate security" to safeguard UCTI. Because this obligation will be contained in the contract itself, the failure to meet the adequate security requirement could have dire consequences for contractors — including breach of contract claims, adverse past performance reports, and even suspension and debarment.

The steps that contractors must take will be determined by the consequences and probability of unauthorized access to the information. "Adequate security" is defined as "protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information."

The regulation specifies that, at a minimum, adequate security requires that the IT systems on which UCTI transits or is stored must comply with specified security standards in NIST Special Publication (SP) 800–53. If a NIST control is not implemented, the contractor must provide a written explanation for the deviation and an explanation of the alternative control or protective measure used to achieve equivalent protection.

NIST controls cover such topics as access control, audit and accountability, training, and system and communications protection. The NIST special publication controls are very similar to the ISO 27002 standard, and thus many larger contractors are likely already in compliance. This may not be the case, however, for smaller companies. This means that contractors may need to work with smaller subcontractors to make sure they are in compliance.

The NIST controls, however, are not a safe harbor. The rule is clear that merely complying with the NIST controls may not be sufficient. The rule provides that contractors must impose other IT system security requirements when the contractor reasonably determines that additional measures "may be required to provide adequate security in a dynamic environment based on an assessed risk or vulnerability."

The NIST controls offer a starting point for contractors. At a minimum, all contractors and subcontractors need to carefully review the NIST standards and ensure both they and their subcontractors apply each of the NIST controls identified in the regulation. As is clear from the regulation, however, the regulation demands that contractors do more: Contractors need to stay aware of new technology and industry best practices and adopt them in their IT systems even before they are given official endorsement by NIST.

Cyber Incident Reports

Under the new cyber incident reporting requirement, all DOD contractors and subcontractors who have UCTI on their IT system, or even 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." Contractors are required to impose the substance of the reporting requirement on their subcontractors.

This cyber incident reporting requirement covers far more activity than intrusions targeted to DOD information. While the final rule limits the type of information covered to UCTI, only rarely do contractors isolate UCTI information on particular IT systems. As such, even intrusions that target other types of information could lead to a reporting requirement if the IT system holds or transits UCTI.

For example, an intrusion targeted only toward personnel or finance information could trigger the need to file a cyber incident report if the UCTI is contained or processed on the same IT system.

And while the rule clearly covers traditional cyber intrusions such as exfiltration through malware, it also would include compromise of the information by employees who download the information without authorization.

In addition to the immediate 72-hour report, the rule imposes additional requirements on contractors in response to an incident, including:

- The contractor must further review its unclassified network for evidence of other incidents of compromise.
- The contractor must identify the specific UCTI that was improperly accessed as a result of the incident.
- The contractor must preserve and protect images of the known affected IT systems and all relevant monitoring/packet capture data for at least 90 days.

In response to a cyber incident report, the DOD has the option of requesting all of the damage assessment information gathered by the contractor, and the contractor has the obligation to comply with these requests unless there is a legal restriction that limits the ability of the contractor to comply.

Given the very short window for meeting the incident reporting requirements, contractors should take steps now to ensure that they can quickly and completely meet all DOD demands. For example, assertions that companies cannot provide data on intrusions to the DOD because of legal requirements will likely be a source of conflict with the DOD. Contractors should address issues of such potential disclosures with those who might have standing to object to complying with this requirement now — before any incident — to ensure that the contractor has the necessary permission to provide the information when requested by the DOD. And contractors should do an inventory of their IT systems to ensure that they fully understand which systems contain UCTI.

Interim Rule on Supply Chain Protection

Out of growing concern that potential adversaries could embed malware in U.S. weapon systems, Congress added Section 806 to the National Defense Authorization Act for Fiscal Year 2011, which authorized the DOD to take action to protect its systems against supply chain risk, which is defined as "the risk than an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a national security system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system."

Section 806 gives the DOD broad authority to take steps to protect against supply side risk, including excluding a source that fails to meet qualification standards or even witholding consent for a contractor to use a particular subcontractor.

As the first step in implementing Section 806, the DOD issued a DFARS interim rule, which implements the DOD's Section 806 authority in several ways. First, it adds a new DFARS subpart 239.73, which provides the process and rules under which the DOD is authorized to:

- Exclude a source that fails to meet qualification standards established in accordance with the requirements of 10 U.S.C. § 2319, for the purpose of reducing supply chain risk in the acquisition of covered systems.
- Exclude a source that fails to achieve an acceptable rating with regard to an evaluation factor providing for the consideration of supply chain risk in the evaluation of proposals for the award of a contract or the issuance of a task or delivery order.

- Withhold consent for a contractor to subcontract with a particular source or direct a contractor for a covered system to exclude a particular source from consideration for a subcontract under the contract.

Several aspects of this subpart are especially worthy of note. First, these authorities are only applicable to the procurement of "covered items" and "covered systems," which are items of information technology purchased for inclusion in a national security system and the loss of integrity of which could result in a supply chain risk for the system.

Second, the exercise of authority is carefully controlled. The authority can only be exercised by the head of the covered agencies — the secretary of defense and the secretaries of the military departments. This authority can only be exercised after obtaining the joint recommendation of the under secretary of defense for acquisition, technology, and logistics and the chief information officer of the Department of Defense, based on a risk assessment by the under secretary of defense for intelligence that there is a significant supply chain risk. And, the authority can only be exercised if there is a determination that the exclusion is necessary to protect national security and less intrusive measures are not reasonably available.

Third, the DOD is allowed to limit the disclosure of information that forms the basis of the exercise of this authority, and any exercise of this authority is not subject to a bid protest in the U.S. Government Accountability Office or federal court.

In addition, the interim rule adds a new contract provision on supply side risk that (1) obligates the contractor to maintain controls in the provision of supplies and services to the government to minimize supply chain risk; (2) notes that the government's exercise of Section 806 authorities is not subject to bid protest, and (3) requires contractors to include the substance of the clause in its contracts with subcontractors.

Looking Ahead: What To Expect in 2014

While last year was certainly one of the most important years for cybersecurity regulation — particularly for DOD contractors — 2014 promises to be a significant year as well.

First, NIST has promised that it will issue its final cybersecurity framework on schedule in mid-February. According to NIST, "The Framework will consist of standards, guidelines, and best practices to promote the protection of critical infrastructure. The prioritized, flexible, repeatable, and cost-effective approach of the framework will help owners and operators of critical infrastructure to manage cybersecurity-related risk while protecting business confidentiality, individual privacy and civil liberties."

While the framework itself is offered as a voluntary set of best practices for cybersecurity, as a practical matter, the framework's standards could soon be mandatory for owners and operators of critical infrastructure:

- In litigation over security breaches, courts will likely look at the standards and best practices in the NIST framework in deciding whether reasonable care was taken by the defendant.
- In exercising their regulatory authority over regulated industries, agencies are likely to look to the framework in setting their own standards.
- The Obama administration is exploring a set of incentives (including access to insurance coverage and limited liability) for those who adopt the best practices to be addressed in the framework.

Second, the FAR Council will issue a new FAR contract provision to govern safeguarding of contractor information systems. A FAR case on this topic was opened in 2011, and a draft rule

was issued in 2012. Comments on this proposed rule have been closed since October 2012, and a final rule is expected sometime next year.

As proposed, the draft rule would add a new contract clause to address requirements for the basic safeguarding of contractor information systems that contain or process information for the government. Unlike the DOD rule on cybersecurity — which applies only to unclassified controlled technical information — the proposed FAR rule would apply to all information generated for the government.

The issuance of the new FAR provision could have large implications for industry. Since the FAR governs a much broader array of government contracts than the DFARS, it could be a significant step toward a broadly applicable set of mandatory cybersecurity requirements. This would be particularly significant if the FAR rule, like the DFARS rule, looked to the controls in NIST Special Publication (SP) 800–53.

Third, there are several other agencies that have either issued new regulations that will be effective in 2014 or may issue new cybersecurity guidance in 2014. For example,

- The Federal Energy Regulatory Commission previously issued its Version 4 Critical Infrastructure Standards, which included a focus on cybersecurity. FERC delayed compliance until October 2014, because it anticipates issuing a Version 5, which will include even more stringent requirements.

- The U.S. Securities and Exchange Commission issued its first guidance on public company disclosure of cybersecurity risks and incidents on Oct. 13, 2011. In May 2003 , the SEC chairman asked the SEC staff to evaluate whether more stringent guidelines are necessary. This analysis could result in new guidance as early as this year.

Cybersecurity legislation has largely gone nowhere because of an inability to come to consensus on the degree to which cybersecurity standards and requirements would be mandatory, and the distrust of the federal government in the wake of the Snowden revelations. In 2013, the DOD demonstrated that mandatory requirements and standards can, through procurement rules, be applied on industry. The pending FAR case and the actions of FERC and other regulatory agencies suggest that 2014 will make this point even clearer.

Charles Blanchard is a partner at Arnold & Porter in Washington, D.C. He previously served as the general counsel of the U.S. Air Force (2009-2013) and general counsel of the U.S. Army (1999-2001).