JONES DAY

JUNE 2015

COMMENTARY

Doing Business with the Government? What You Should Know about Cybersecurity

Government contractors are in a difficult position when it comes to cybersecurity. Not only do they need to worry about cybersecurity issues that affect almost every company, but they also often house sensitive government data that can carry additional obligations. Further, the very fact that they have access to this information, and their relationship to the U.S. government, makes them an attractive target for malicious efforts. Escalating these concerns, not only are contractors with sensitive information prime targets for standard hackers trying to prove their worth, but they are also in the cross-hairs for attacks sponsored by countries hostile to the United States or interested in obtaining technology otherwise prohibited to them.

The U.S. government recognizes this threat and has responded in two major ways. The first is to impose additional cybersecurity responsibilities on contractors who have access to sensitive data. While the goal of these additional obligations is to harden security to protect data, their parameters are not always apparent and can be easily misunderstood. Just identifying what a contractor is expected to do can be a challenge. The second element of the government's approach is to assist in combating cyber attacks by offering to work with companies, including contractors, who find themselves victims. This help can be invaluable, especially for sophisticated and persistent state-sponsored cyber threats. It also raises additional issues, however, and many companies are justifiably suspicious of opening their information technology systems to the government.

In this *Commentary*, we highlight the aligned and competing priorities of the government and companies in this space. We discuss some of the main requirements imposed on contractors that go above and beyond those required of standard companies. We also delve into practical considerations for government contractors in this area and developing trends.

Baseline Requirements

As government contractors sit at the intersection of private commerce and public service, they are subject to commercial and government requirements. The data held in their computer networks may include personal information on customers and employees, and sensitive information related to government programs. In the wake of massive intrusions and compromises of data at major retailers and health insurers, much of the media attention and legislative action regarding cybersecurity has been targeted at protection and reporting of security breaches relating to personal

information.[1] The government, however, also imposes requirements above and beyond these obligations. The type and level of restrictions a company must implement due to sensitive government information depend in large part on the nature of the information.

Classified Information. The most obvious and longest standing set of obligations relates to classified information. Contractors must obtain a security clearance from the U.S. government before they can access classified materials or information. This clearance includes one for the contractor (facility clearance) and clearances for any employee accessing classified materials (personnel clearances). This involves compliance with an extensive set of requirements outlined in the National Industrial Security Program Operating Manual ("NISPOM"). Compliance with the NISPOM can be demanding and can require extensive changes to the IT system of a company (among other obligations) to ensure that no individuals without a clearance have access to classified materials. Contractors must meet certain "baseline standards" established by the Defense Security Service Office of Designated Approving Authority ("DSS ODAA") relating to information systems used to process classified information. Once these standards are met, a contractor may certify and submit the system to DSS ODAA for approval and accreditation. Information systems must be accredited prior to processing classified information.

Controlled Information. One of the most widely misunderstood requirements of securing government information is the fact that entities must still take steps to protect government data even if that data is not classified. These obligations originate from several sources, from agency-specific requirements, to export controls, to newer requirements imposed on "unclassified controlled technical information" ("UCTI").[2] Information security requirements can be found in Federal Acquisition Regulation ("FAR") clauses requiring confidentiality. They can also be found in agency-specific contract clauses that differ from the standard FAR requirements. In addition, even if a contract does not include any provisions requiring the safeguarding of information, if technical data or other information is controlled under the International Traffic in Arms Regulations ("ITAR"), Export Administration Regulations ("EAR"), or similar regimes, then a contractor must ensure that the material is not accessed by prohibited individuals or entities. In the case of ITAR-controlled information, this could include any foreign national, *even if the transfer takes place in the United States*. EAR and other regulatory schemes can be similarly restrictive.

From a cybersecurity perspective, protection of UCTI remains a patchwork of agency-specific cybersecurity requirements and reporting procedures. For example, the General Service Administration ("GSA") has one of the more comprehensive contract clauses addressing cybersecurity. GSA Acquisition Regulation 552.239-71 is an agency-unique requirement that applies to unclassified IT resources and requires government contractors to submit an IT security plan that complies with the Federal Information Security Management Act and other federal requirements. It also requires specific warnings alerting users accessing GSA information and a "continuous monitoring plan."

In a similar vein, the Department of Defense ("DOD") requires its contractors to take certain measures to protect "UCTI" pursuant to Defense Federal Acquisition Regulation Supplement ("DFARS") Subpart 204.73. Contract clause 252.204-7012, "Safeguarding of Unclassified Controlled Technical Information," details requirements to be included in every DOD contract and subcontract involving UCTI. These regulations outline the minimum required National Institute for Standards and Technology ("NIST") security controls that a contractor must implement in its information technology system. The system must employ, at a minimum, NIST security controls listed in Special Publication 800-53 relating to: (i) access control, (ii) awareness and training, (iii) audit and accountability, (iv) configuration management, (v) contingency planning, (vi) identification and authentication, (vii) incident response, (viii) maintenance, (ix) media protection, (x) physical and environmental protection, (xi) program management, (xii) risk assessment, (xiii) systems and communication protection, and (xiv) system and information integrity. The DFARS provision also requires that contractors mark UCTI with specified distribution statements. The intelligence community has begun to incorporate similar safeguard requirements as well.

At present, the government is attempting to standardize the approach to UCTI. In May 2015, the National Archives and Records Administration's ("NARA") Information Security Oversight Office ("ISOO") issued a proposed rule to "establish

policy for agencies on designating, safeguarding, disseminating, marking, decontrolling, and disposing of" UCTI.[3] ISOO explained that this rule is the first of a three-step process to streamline procedures into a uniform set of requirements. The next step is for ISOO to work with NIST to "develop a special publication on applying the information systems security requirements in the contractor environment."[4] Working in tandem with NARA, NIST is developing Special Publication 800-171, "Protecting Unclassified Information in Nonfederal Information Systems and Organizations." This publication will focus on many of the same things as the DFARS 7012 clause, but they are not identical. The third and final step referenced by NARA is for ISOO to develop a single FAR clause "that will apply the requirements of the proposed rule" to contractors.[5] Because the requirements of the GSA, DOD, and NARA clauses are all different, until the government clearly establishes a uniform standard, contractors will need to monitor the requirements of their actual agreements to determine their obligations.

Mandatory Reporting of Cyber Incidents and Data Breaches

Most states and certain federal agencies have implemented mandatory reporting of cyber incidents and data breaches.[6] At the state level, these laws require notification of breaches involving defined personal information. In many cases, the state legislation has a safe harbor that eliminates reporting requirements or reduces potential penalties if certain best practices have been followed—for example, encrypting the data. As with the cybersecurity protective measures described above, government contractors must meet the commercial reporting requirements required of all businesses as well as those imposed by the government agencies with which they contract.

The DOD requires immediate reporting and provides no safe harbor. Under the DFARS clause, defense contractors have 72 hours to report cyber incidents involving any unauthorized access to, or any possible exfiltration, manipulation, or other loss or compromise of, UCTI on or transiting unclassified information systems. Prime contractors must also report incidents involving their subcontractors' information systems. In addition, the contractor must conduct a further review of the breach and maintain images of the known affected systems for at least 90 days to allow DoD time to request the information. Similar to above, contractors in the intelligence community are also finding themselves subject to immediate reporting requirements.

Congress is also considering legislation relating to companies' ability to share information relating to cybersecurity threats and attacks. Two of the more prominent bills, the Protecting Cyber Networks Act (HR-1560) and the National Cybersecurity Protection Advancement Act of 2015 (H.R. 1731), focus on authorizing companies to share among each other and with the U.S. government. These bills seek to provide some protection to these companies in the form of shielding them from liability that could arise from such sharing. The stated goals of these bills are to encourage the collection and analysis of cyber threats information so that the private and public sector can benefit from a larger pool of knowledge and a unified approach.

Government Response and Resources

The U.S. government has identified cybersecurity as a major issue affecting national interests. Speaking about cybersecurity in his 2015 State of the Union address, President Obama emphasized that "we cannot look back years from now and wonder why we did nothing in the face of real threats to our security and our economy."[7] The U.S. government has acknowledged that U.S. entities need help in fending off these attacks. As John Carlin, Assistant Attorney General for National Security, noted, "it's not fair to let the private sector" face threats from nation-states "alone."

The government has indicated that it is willing to use a wide variety of its tools in combating this threat. These take two main forms. The first is the arsenal of offensive means the government possesses to pursue offenders. This includes individual prosecutions. It also includes the power to levy sanctions, block transactions, and freeze assets to counter individuals and efforts by nations. To this effect, the government recently created the Cyber-related Sanctions program.[8] This program authorizes the government to impose sanctions on individuals and entities involved in the disruption of critical infrastructure sector networks or misappropriation of funds, economic resources, trade secrets, personal identifiers, or

financial information "for commercial or competitive advantage or private financial gain."[9]

The Pentagon has also recognized the importance of mobilizing against cybersecurity threats. In late April 2015, DOD Secretary Ash Carter announced the DOD's new cyber strategy. This strategy focuses on defending DOD networks, systems, and information; defending against "significant" cyber attacks; and providing cyber capabilities to military operations. One important aspect of this strategy is the acknowledgment that offensive cyber will be considered an option to increase deterrence of future cyber attacks against American interests. Using these resources can go a long way toward providing a defense for government assets and those of the companies that work with the government.

The government also performs the important task of collecting and consolidating information regarding cyber attacks, private and state-sponsored. This information is useful in establishing countermeasures to help defend against attacks. The government has recognized, however, that it needs to encourage the sharing of this information within the government and between industry and government. As a result, recent government efforts have centered around the formation of various bodies designed to improve the sharing of cyber threat information and intelligence. On February 13, 2015, Executive Order 13691 noted that "sharing information related to cybersecurity risks and incidents play[s] an invaluable role in the collective cybersecurity of the United States."[10] The Order requires the Department of Homeland Security to encourage the formation of Information Sharing and Analysis Organizations ("ISAOs") as a voluntary information-sharing framework for public and private sector collaboration. In a February 25, 2015, memorandum to various agency heads, the President ordered the establishment of the Cyber Threat Intelligence Integration Center ("CTIIC") under the Director of National Intelligence. The CTIIC will be an interagency organization dedicated to developing intelligence on foreign cyber threats and disseminating the information to U.S. government and private sector entities. It is tasked with ensuring that intelligence regarding malicious cyber activity and threat reports are downgraded to the lowest classification possible for distribution within government and to private entities.

Practical Considerations

As one of the most active areas of policy development, government contractors will need to maintain nimble cybersecurity policies and procedures. To better prepare for cyber threats—and the government regulations aimed at protecting its sensitive data—contractors need to understand the obligations that each of the customer agencies imposes on the government contractor.

Until the goal of harmonized government-wide regulations is realized, this will likely mean a patchwork of requirements with potentially significant differences in implementation details. The absence of a unified government response could force contractors to be overinclusive in adopting compliance measures, potentially resulting in an inefficient allocation of resources. Contractors to the defense and the intelligence communities have already had to implement policies to meet the recent contractual requirements. Because of the administration's continued focus on cybersecurity, we expect the pace of implementation of requirements in other agencies to increase. As a result, prudent government contractors, even those doing business with agencies without specific cybersecurity requirements, should begin to adopt NIST security controls.

Any cybersecurity program will have costs associated with these requirements. Modifying IT systems to comply with NIST standards will certainly increase the amount of resources that companies need to devote to compliance. In addition, while contractors will benefit from effective threat intelligence sharing, the formation of government information-sharing organizations may be a double-edged sword. An example of this is the Presidential Memorandum directing member agencies of the CTIIC to provide it with all intelligence related to foreign cyber threats or incidents. To carry out this order, those agencies will likely increase oversight of cybersecurity of its contractors and mandate reporting through their acquisition regulations, like those established by the DFARS 7012 clause. Further, the requirements that accompany breach reporting and data retention also carry underlying costs. Depending on the size of the breach, mandates to retain relevant data could require contractors to purchase or lease new storage capacity to properly maintain images of breached systems while preserving the ability to conduct day-to-day business.

Although every contractor must have protections in place to prevent industrial espionage of trade secrets and other intellectual property that contributes to the business's assets, some contractors—especially small business subcontractors—may not have the ability to defend against state-sponsored cyber espionage. The government should weigh the costs of these measures against the ability of contractors to comply with them. While security is important, increasing requirements may become untenable, especially for smaller subcontractors, and the government should avoid ultimately reducing the industrial base available for government purposes.

Contractors must also carefully weigh their options in seeking to partner with the government concerning breaches. While assistance in combating an attack will likely prove useful (if not essential), companies must consider whether they are creating exposure by opening the door to enforcement agencies. The government has indicated (informally and in the rule-making process) that it will limit use of information gathered during defense of cyber attacks. Recently, the Department of Justice has emphasized that it is not interested in prosecuting victims of hacking as incompetent protectors of data but, rather, on preventing breaches from occurring. In addition, pending legislation contains protections for companies for liability that may arise from the act of sharing information relating to a cyber threat. This is a developing area, however, and there are no guarantees that the government will not pursue leads it discovers through breach reports or activities it undertakes with companies that have been subject to a cyber attack.[11] In addition, the interests of companies will not always align with the government. For example, while most companies will simply want the attack to stop, the government may be more interested in tracking down the perpetrators. For many companies, reporting will not be an option due to mandatory provisions and for some companies, the benefits may outweigh any risks. Despite this, companies should carefully consider how far beyond mandatory reporting they wish to go.

Conclusion

As entities that work with the government in some of the most critical and sensitive areas, it is not surprising that government contractors have an additional set of concerns relating to information and data security. The need to track an additional set of compliance requirements, not to mention devote resources to them, will likely cause headaches at companies. The future almost certainly holds increased requirements in this area. Contractors that take a proactive approach to these requirements, however, will be able to develop efficient measures to ensure compliance. Further, if done correctly, they will likely be able to use these security measures to differentiate themselves from other contractors and develop a competitive advantage.

Lawyer Contacts

For further information, please contact your principal Firm representative or one of the lawyers listed below. General email messages may be sent using our "Contact Us" form, which can be found at www.jonesday.com/contactus/.

Peter F. Garvin III
Washington
+1.202.879.5436
pgarvin@jonesday.com

Jeff Rabkin
San Francisco
+1.415.875.5850
jrabkin@jonesday.com

J. Andrew Jackson
Washington
+1.202.879.5575
ajackson@jonesday.com

Grant H. Willis
Washington
+1.202.879.3847
ghwillis@jonesday.com

Fernand A. Lavallee
Washington
+1.202.879.3486
flavallee@jonesday.com

D. Grayson Yeargin
Washington
+1.202.879.3634
gyeargin@jonesday.com

Todd S. McClelland
Atlanta
+1.404.581.8326
tmcclelland@jonesday.com

Chad O. Dorr
Washington
+1.202.879.3795
cdorr@jonesday.com

Mauricio F. Paez
New York
+1.212.326.7889
mfpaez@jonesday.com

Endnotes

1 For example, among the first actions by the 114th Congress was the introduction of bills aimed at mandatory reporting of cybersecurity incidents. *See* Data Security Breach and Notification Act of 2015, S.177, introduced January 13, 2015; Cyber Privacy Fortification Act of 2015, H.R. 104, introduced January 6, 2015.

2 The government also references UCTI as "controlled unclassified information" ("CUI").

3 80 FR 26501.

4 80 FR 26503.

5 *Id.*

6 For updates on changing state data breach notification requirements and other laws, see the Jones Day *Global Privacy & Cybersecurity Update* located on the Jones Day Cybersecurity, Privacy, & Data Protection practice publication page.

7 Jones Day previously commented on this in the February 2015 *Global Privacy & Cybersecurity Update*, Issue 5.

8 Jones Day previously discussed this program in the May 2015 *Global Privacy & Cybersecurity Update*, Issue 6.

9 Executive Order 13694, "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities," 80 Fed. Reg. 18077 (Apr. 2, 2015).

10 For additional information on Executive Order 13691, please read our *Commentary*, "President Obama Continues Push on Cybersecurity."

11 For instance, the DFARS provides that information obtained "may be used to support an investigation and prosecution of *any* person or entity …."