Client Advisory

pillsbury

Privacy, Data Security & Information Use

Cybersecurity Assessment

National Security

Government Contracts & Disputes

Cybersecurity Task Force

February 2, 2016

Government Contractors Brace For Continuing Changes in Cybersecurity Regulations

By C. Joël Van Over, Brian P. Cruz and Travis L. Mullaney

The federal government has responded to recent data breaches by making cybersecurity a top priority, and it continues to consider and implement a number of regulations that affect government contractors.

Over the past year and a half, the Office of Personnel Management (OPM) suffered two massive data breaches that collectively exposed the records of approximately 22.1 million people both inside and outside the federal government, including information pertaining to both current and former federal employees as well as their families.[1] The stolen information includes an extensive trove of Personally Identifiable Information collected from security clearance applications known as SF-86 forms, with hackers gaining access to everything from Social Security numbers to fingerprints.[2]

The OPM hack followed shortly after a string of other recent high-profile federal data breaches, including the exploit of a feature on the Internal Revenue Service website that allowed access to the tax forms of more than 330,000 people[3] and the unauthorized access of recently unclassified email systems in use at both the Pentagon[4] and the White House.[5] These federal data breaches are part of a larger trend of suspected state-sponsored attacks that also includes a major hack of Sony Pictures Entertainment in November of 2014 that exposed employees' personal information, emails and executive salaries, among other information.[6] Even where foreign government actors have not been implicated, we have seen hugely damaging information dumps from well-known companies such as Target, Home Depot, and J.P. Morgan[7] as well as the widely discussed hack of extra-marital matchmaker Ashley Madison.[8]

The threat of increasingly sophisticated cyber-warfare has and will continue to prompt cybersecurity entrepreneurs, vulnerable industries (recent research has exposed vulnerabilities in everything from cars[9] to rifles[10]), the federal government and NATO[11] to invest in new technologies and best practices. Given the ease with which digital information can be transmitted and the continuing proliferation of new technologies riding quietly on the internet or being developed and stored in cloud-based systems, the federal government has responded to the threats these technologies pose by making cybersecurity a top priority.[12] The recent enactment of the Cybersecurity Act of 2015, allowing for greater sharing of cyber threat information between governmental and private entities, further evidences the growing concern in

Washington.[13] To improve cybersecurity, the federal government has begun to roll out a number of regulations and policies that will affect federal contractors in the coming months.

OMB Considers Public Comments on Improving Cybersecurity Protections in Federal Acquisitions

Acknowledging the dramatic increase in threats facing federal information systems as agencies move to provide more services online, the Office of Management and Budget (OMB) Office of E-Government & Information Technology (E-Gov) recently sought public comment on its draft guidance to improve cybersecurity protections in federal acquisitions.[14] The OMB's authority derives from updates to the Federal Information Security Modernization Act (FISMA) in 2014, OMB policy, and standards promulgated by the National Institute of Standards and Technology (NIST), which collectively provide a framework for securing government and contractor information systems. FISMA, for example, "requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source."[15] The ultimate goal of OMB's draft guidance is therefore to better protect information stored on government information systems, contractor information systems, and contractor information systems that are part of an IT service operated on behalf of the federal government.

OMB's memorandum of proposed guidance includes the following recommendations:

1. **Security Controls**
    - For systems operated on behalf of the government, agencies must require the contractor system to meet the appropriate baseline in NIST SP 800-53 as modified by the agency to meet its risk management requirements.
    - For contractors' internal systems used to provide a product or service for the government but incidentally containing Controlled Unclassified Information (CUI), agencies must require contractors to meet the requirements of NIST SP 800-171 rather than NIST SP 800-53.
2. **Cyber Incident Reporting**
    - A "cyber incident" is defined as "actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein."
    - Agencies must include minimum contract language specifying to whom, what, when, and where cyber incidents should be reported along with consequences of non-compliance.
3. **Information Systems Security Assessments**
    - Agencies are tasked with assessing the impact level of the data that is to reside in the contractor's information system in order to determine what types of controls should be applied, followed by determining whether it is appropriate to obtain an independent security assessment.
    - Agencies may accept independent third-party verification of security assessment results, as well as contractor or government assessment evidence, based on their risk assessments.

- Contractors must afford the agency access to the contractor's facilities, installations, operations, documentation, databases, IT systems, devices and personnel used in performance of the contract, regardless of location, to the extent required to conduct an inspection, evaluation, investigation or audit and to preserve evidence of information security incidents.

4. **Information Security Continuous Monitoring (ISCM)**

   - ISCM is defined by reference to NIST requirements "as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions."

   - Agencies may utilize the Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) program to obtain much of the information required for ISCM. If, however, the agency determines that providing the DHS CDM capabilities to a contractor operating information systems on behalf of the government is not feasible, the contract must ensure that at a minimum:

     - Contractor-operated systems meet or exceed the information security continuous monitoring requirements identified in M-14-03; and

     - The agency may elect to perform information security continuous monitoring and IT security scanning of contractor systems with tools and infrastructure of its choosing.

   - For systems not operated on behalf of the government – contractor's internal systems used to develop a product or service – continuous monitoring is part of the security assessment requirement in NIST SP 800-171.

5. **Business Due Diligence**

   - Agencies are also tasked with conducting reasonable business due diligence while making use of GSA's business due diligence information shared service, which provides access to risk information that encompasses data collected from voluntary contractor reporting, public records, publicly available and commercial subscription data based on transparent, objective and measurable risk indicators.[16]

In addition to the requirements noted above, agencies are also tasked with continual review of contract activities to ensure that OMB guidance is applied. Agencies are encouraged to use security assessments to confirm that contractors are maintaining their security posture and to allow the agency to validate the maintenance of previously performed independent assessments. Should an agency determine that a contractor is not performing in accordance with the guidelines, agencies are empowered to take performance problems of predecessor firms and key employees into account when selecting vendors during the procurement process.

OMB's guidance is expected to be finalized in the coming months. Contractors may wish to consult with an attorney in advance to ensure relevant compliance procedures are in place.

OMB's memorandum of proposed guidance on improving cybersecurity in acquisitions is just one component in a broader cybersecurity plan, however. In October of last year, OMB also issued a

memorandum outlining its broader Cybersecurity Strategy and Implementation Plan (CSIP) for the federal civilian Government centering around five principal objectives:

1. **Prioritized identification and protection of high value information and assets;**
2. **Timely identification of and rapid response to cyber incidents;**
3. **Rapid recovery from incidents when they occur and accelerated adoption of lessons learned;**
4. **Recruitment and retention of the most highly-qualified cybersecurity workforce talent the federal government can bring to bear; and**
5. **Efficient and effective acquisition and deployment of existing and emerging technology.**

The objectives of the CSIP will undoubtedly shape and define agency policies and procedure pertinent to contractors in the coming years. At least two of the objectives will likely directly affect contractors right away. First, in order to protect high value information, OMB is recommending implementation of strong authentication Personal Identify Verification (PIV) credentials for employees and contractors with access to such information. Current targets seek the implementation of 100% PIV for privileged users and 75% PIV for non-privileged users. Second, the CSIP's objective of efficient and effective acquisition and deployment of existing and emerging technology will require close partnerships with contractors to continue implementing cybersecurity solutions already underway and on the horizon. There may be significant opportunities for contractors to leverage experience in this area into new work.

DoD Presses Interim Regulations that Substantially Broaden the Scope of Defense Contractor and Subcontractor Cybersecruity Compliance Obligations, Enhance Cyber Incident Reporting and Acquisition of Cloud Computing Services

In August of last year, the Department of Defense (DoD) issued an interim regulation substantially expanding the existing Defense Federal Acquisition Regulation Supplement (DFARS) provisions requiring contractors to safeguard "Covered contractor information systems" and "Covered defense information" and to report "Cyber incidents." The regulation also clarifies DoD policy regarding the acquisition of cloud computing services.[17] The interim rule was put into effect without an opportunity for public comment, based on urgent and compelling circumstances, but the interim rule was almost immediately criticized for implementing significant and costly changes.[18] For example, the interim regulations effectively adopt the NIST Special Publication (SP) 800-171 security requirements ("NIST SP 800-171") (in effect on the date the solicitation is issued) as baseline security requirements, in conjunction with the Cloud Computing Security Requirements Guide (SRG) (in effect on the date the solicitation is issued) and the provisional authorization (accreditation) required by the Defense Information Services Agency ("DISA") to the extent cloud computing services are used in the performance of a DoD contract or are acquired expressly as a service by DoD. Compliance with these requirements will not only be costly for most federal contractors and subcontractors, but will take time to evaluate, implement, and assess operationally. Other criticism of the interim regulations focused on the breadth of the definitions of terms used in the regulation, including those that relate to the definition of a Cyber incident and the mandatory "rapid" reporting of such incidents. These criticisms include the inherent vagueness in the obligation to report "potentially adverse effects" to information systems, and the potential costs required to preserve and protect images of affected systems for several months. The most significant changes dictated by the interim rule include the following:

1. **Cyber Security Compliance and Incident Reporting**
   - DFARS 252.204-7012
     - Mandates "adequate security" "for all covered defense information on all covered contractor information systems that support the performance of work" under the contract, and specifies adequate security requirements as defined in NIST SP 800-171 and requires reporting of any such security requirements not implemented at the time of contract award, or the identification of alternative equivalent security measures approved by DoD when unable to satisfy NIST SP 800-171 requirements, in accordance with DFARS 252.204-7008.
     - Mandates the robust investigation and reporting of cyber incidents and specifies "rapid" 72-hour reporting and minimum reporting elements.
     - Mandates the delivery of isolated malicious software in accordance with instructions from DoD.
     - Mandates a flow-down of clause to all subcontractors, with no exceptions for small business or commercial items.
     - Requires affirmative cooperation with post-report investigations, including preserving images of all affected systems for 90 days.
   - DFARS 252.204-7009
     - Mandates conditions for handling and protecting information obtained from a third-party's reporting of a cyber incident and specifies potential penalties for the breach of these conditions.
   - DFARS 252.204-7008
     - Mandates the procedures required for a contractor to justify and obtain DoD approval for alternative security measures that do not comply with NIST SP 800-171.
2. **Cloud Computing Services**
   - DFARS subpart 239.76
     - Establishes the DoD policy for the acquisition of cloud computing services.
   - DFARS 252.239-7009
     - Requires offerors to check a box indicating whether it intends to use cloud computing services in the performance of the contract or a subcontract.
   - DFARS 252.239-7010
     - Defines "Cloud Computing" other relevant terms and mandates security requirements in accordance with the Cloud Computing Security Requirements Guide in effect when solicitation issued and mandates cyber incident reporting, preservation and cooperation in post-incident analysis.
     - Mandates a flow-down of clause to all subcontractors, with no exceptions for small business or commercial items, if subcontract "may involve cloud services".

Following discussions at a public meeting held on Monday December 14, 2015, the DoD issued a revised interim regulation on December 30, 2015 that pushed back mandatory implementation of NIST SP 800-171 standards until December 31, 2017.[19] Comments on the revised interim rule are due February 29, 2016, and we encourage affected federal contractors and subcontractors to consider submitting

comments.[20] While, the revised interim regulation does not require immediate full compliance with NIST SP 800-171 until December 31, 2017, the revised interim regulation does require contractors (and affected subcontractors) to identify those aspects of its system that do not comply the NIST standards on the date the solicitation is issued ("or as authorized by the Contracting Officer), and to identify alternative measures implemented to secure protections contemplated by the NIST standards and to follow specific procedures for securing approval from DoD for such alternative measures. As the revised interim rule has already been placed into effect as part of the current DFARS, contractors should expect to see the clauses included in forthcoming solicitations.

Insider Security Threats Spur Significant Changes to NISPOM – the Federal Government's Rule Book on Protecting Classified Information

As we have seen from recent insider intelligence leaks *à la* Chelsea Manning and Edward Snowden, cybersecurity threats need not originate from external actors. Threats like these have placed the federal government on high alert, requiring contractors handling classified information to remain on high alert as well. Among other things, the federal government is requiring such contractors to strengthen their internal controls by establishing their own insider threat programs designed to protect classified information from unauthorized disclosure. Final guidance on what form such programs must take is expected to arrive shortly in the forthcoming "Conforming Change No. 2" to the National Industrial Security Program Operating Manual (NISPOM). Contractors handling classified information may wish to begin planning and implementation now, since the contours of the requirements that will form the foundation of Conforming Change No. 2 are reasonably clear. In addition, numerous industrial security letters have been issued (and rescinded) by the Defense Security Service, effectively amending or affecting Chapter 8 (Information System Security) of the NISPOM,[21] and contractors subject to the NISPOM should be updating their compliance with these security letters.

The history of the anticipated changes to the NISPOM dates back to October 7, 2011, when President Obama signed Executive Order 13587 directing structural reforms to improve the security of classified networks and to ensure responsible sharing and safeguarding of classified information. Executive Order 13587 both established an Insider Threat Task Force and mandated that federal agencies with access to classified computer networks implement their own insider threat detection and prevention programs. The requirements of Executive Order 13587 were later clarified in a November 2012 Presidential Memorandum entitled "National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs." This Presidential Memorandum set forth specific guidelines for agencies to use in developing their own insider threat programs and was later implemented on September 30, 2014 via DoD Directive 5205.16.

Among the directives laid out in DoD Directive 5205.16 is the requirement that the Under Secretary of Defense for Acquisition, Technology, and Logistics develop policy or amend the DFARS and develop contract clauses "to ensure DoD contracts impose uniform insider threat program requirements." The DoD has since announced that the amended regulations will arrive in Conforming Change 2 to the NISPOM, codified at DoD 5220.22-M, which sets the mandatory structural and process requirements for the protection of classified information to which properly cleared federal contractors and their employees have access in connection with classified contracts under the National Industrial Security Program (NISP).

Conforming Change No. 2 will outline insider threat requirements for cleared industry operating under the NISP. The DoD's advance notice to industry indicates that the minimum standards will require thoughtful implementation and vigilance, including:

1. Establishment of an insider threat program
2. Designation of an insider threat senior official who is cleared in connection with the facility clearance
3. Self-assessment of insider threat programs
4. Provision of training for insider threat program personnel and awareness for employees
5. Monitoring of network activity

If Conforming Change No. 2 follows the Minimum Standards set forth in the November 2012 Presidential Memorandum, contractors may be faced with a 180-day timeline to establish and implement an insider threat program in accordance with the standards outlined above. Further, contractors will likely be required to maintain records necessary to identify, analyze, and resolve insider threat matters, including keeping records and actively monitoring the following general categories of information more systematically:

- Counterintelligence and Security: Relevant databases and files including but not limited to, personnel security files, polygraph examination reports, facility access records, security violation files, travel records, foreign contact reports and financial disclosure filings.

- Information Assurance: Relevant network information including, but not limited to, personnel usernames and aliases, levels of network access, audit data, unauthorized use of removable media, print logs, and other data needed for clarification or resolution of an insider threat concern.

- Human Resources: Relevant HR databases and files including, but not limited to, personnel files, payroll and voucher files, outside work and activities requests, disciplinary files, and personal contact records, as may be necessary for resolving or clarifying insider threat matters.

Contractors may also be required both to establish procedures for handling access requests by the insider threat program involving particularly sensitive or protected information and to establish reporting guidelines to refer relevant insider threat information directly to the insider threat program.

Although we will know more once Conforming Change No. 2 is issued, it is certain that robust changes will be required in areas that may not have been the subject of systematic scrutiny in the past. In sum, most contractors have not yet contemplated or adopted an insider threat program based upon their specific organizational and operational risk profile and requiring senior management involvement. Accordingly, it would be prudent for contractors that handle classified information to begin preparing for the coming changes now. Specifically, prime contractors and subcontractors with cleared facilities and with employees who hold security clearances and who have access to classified information may wish to be proactive in developing policies and protocols designed to assess internal threats and to detect and manage these threats. Demonstrating compliance, and therefore limiting risk, will depend upon an effective threat analysis, prioritizing risks, effectively maintaining and monitoring relevant data, and adopting measures designed to mitigate or eliminate potential threats from within a contractor's organization, and taking appropriate action if a breach is detected.

Agencies Are Seeking Proposals for Implementing Cybersecurity and Insider Threat Programs

In conjunction with the additional cybersecurity requirements being imposed upon agencies, the federal government has been seeking contractor assistance in implementing the regulations.

In spring of last year, the Defense Information Technology Contracting Organization issued a $475 million Request for Proposals (RFP) seeking to buttress staffing at the U.S. Cyber Command with the aid of private contractors.[22] Although this solicitation was later cancelled, the government has indicated its intent to "reassess the needs of USCYBERCOM and to consider whether another acquisition strategy could better meet those needs."[23]

USCYBERCOM is not the only federal organization seeking contractor help with cybersecurity matters. In August of last year, the Air Force similarly sought proposals from contractors to develop an insider threat monitoring implementation plan, manage the insider threat program, develop metrics to track program implementation progress, and coordinate with stakeholders to determine Air Force capabilities to address insider threat issues.[24] Although the Air Force solicitation has now closed, there is every expectation that similar RFPs will issue from other agencies down the road. Therefore, contractors seeking to perform work in these areas should remain vigilant in monitoring the issuance of similar solicitations in the near future.

Federal Government Continues Implementation of FedRAMP Program to Provide a Standardized Approach to Security Assessment, Authorization, and Continuous Monitoring for Cloud Products and Services.

In late 2011, the OMB issued a memorandum directing the development and implementation of the Federal Risk and Authorization Management Program (FedRAMP) in order to introduce a policy approach to developing trusted relationships between executive departments and agencies and cloud service providers.[25] As implemented, FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.[26] In developing FedRAMP, cybersecurity and cloud computing experts from numerous agencies, including General Services Administration (GSA), NIST, DHS, DoD, National Security Agency (NSA), OMB, the federal CIO Council and its working groups, collaborated with private industry groups to create a workable set of standards and requirements for securely utilizing cloud solutions.[27]

As a starting point, FedRAMP requires prospective cloud service providers (CSPs) seeking to do business with the government to initiate an assessment process and/or security authorization using the FedRAMP requirements, which are FISMA-compliant and based on the NIST 800-53 rev3 standards.[28] Once the CSPs have implemented the FedRAMP security requirements on their environment, they must hire a FedRAMP-approved third party organization to perform an independent audit of the cloud system so as to provide a security assessment package for review.[29] The FedRAMP Joint Authorization Board then reviews the security assessment package and determines whether to grant a provisional authorization.[30]

Ultimately, FedRAMP authorization of cloud systems is a three-step process involving:

1. **Security Assessment**
   - The security assessment process uses a standardized set of requirements in accordance with FISMA using a baseline set of NIST 800-53 controls to grant security authorizations.
2. **Leveraging and Authorization**
   - Federal agencies view security authorization packages in the FedRAMP repository and leverage the security authorization packages to grant a security authorization at their own agency.
3. **Ongoing Assessment & Authorization**
   - Once an authorization is granted, ongoing assessment and authorization activities must be completed to maintain the security authorization.[31]

As the forms and processes of FedRAMP can prove daunting, contractors requiring assistance in navigating the regulatory compliance framework may consider seeking attorney guidance to facilitate the process and the protection of the sensitive information that must be revealed to achieve authorization under FedRAMP.

If you have any questions about the content of this alert, please contact the Pillsbury attorney with whom you regularly work, or the authors below.

Joël Van Over (bio)
Northern Virginia
+1.703.770.7654
joel.vanover@pillsburylaw.com

Brian P. Cruz (bio)
Los Angeles
+1.213.488.7101
brian.cruz@pillsburylaw.com

Travis L. Mullaney (bio)
Northern Virginia
+1.703.770.7751
travis.mullaney@pillsburylaw.com

[1] Ellen Nakashima, *Hacks of OPM databases compromised 22.1 million people, federal authorities say*, Federal Eye, The Washington Post (July 9, 2015), https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/

[2] *See id.*

[3] *See* Jose Pagliery, *IRS says criminals actually stole data on 330,000 – three-times more than previously believed*, CNN Money: Cyber-Safe (Nov. 19, 2015), http://money.cnn.com/2015/08/17/technology/irs-data-theft/index.html.

[4] *See* Jamie Crawford, *Russians hacked Pentagon network, Carter says*, CNN Politics (June 4, 2015), http://www.cnn.com/2015/04/23/politics/russian-hackers-pentagon-network/.

[5] *See* Evan Perez and Shimon Prokupecz, *How the U.S. thinks Russians hacked the White House*, CNN Politics April 8, 2015), http://www.cnn.com/2015/04/07/politics/how-russians-hacked-the-wh/.

[6] *See* Edgar Alvarez, *Sony Pictures hack: the whole story*, Engadget, (Dec. 10, 2014) http://www.engadget.com/2014/12/10/sony-pictures-hack-the-whole-story/; *see also* Andrea Peterson, *The Sony Pictures hack, explained*, The Switch, The Washington Post (Dec. 18, 2014), https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/.

[7] *See* Keith Collins, *A Quick Guide to the Worst Corporate Hack Attacks*, Bloomberg (Mar. 18, 2015), http://www.bloomberg.com/graphics/2014-data-breaches/.

[8] *See* Robert Hackett, *What to know about the Ashley Madison hack*, Fortune (Aug. 26, 2015), http://fortune.com/2015/08/26/ashley-madison-hack/.

[9] *See* Andy Greenberg, *Hackers Remotely Kill a Jeep On the Highway – With Me In It*, WIRED (July 21, 2015), http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

[10] *See* Andy Greenberg, *Hackers Can Disable A Sniper Rifle – Or Change Its Target*, WIRED (July 29, 2015), http://www.wired.com/2015/07/hackers-can-disable-sniper-rifleor-change-target/.

[11] *See* North Atlantic Treaty Organization, *Cyber Security* (Nov. 25, 2015), http://www.nato.int/cps/en/natohq/topics_78170.htm

[12] *See Statement by DHS Secretary Jeh C. Johnson on the Federal Cybersecurity Enhancement Act of 2015* (July 30, 2015) ("Cybersecurity is a top priority for me, for the President, and for this Administration. I am pleased that Congress has recognized that we need to work together to ensure that we have adequate resources and budget, and the legal authorities necessary to pursue the mission."), *available at* http://www.dhs.gov/news/2015/07/30/statement-secretary-jeh-c-johnson-federal-cybersecurity-enhancement-act-2015 (last accessed Jan. 11, 2015).

[13] *See* Tom Risen, *Obama Signs Cybersecurity Law In Spending Package*, U.S. News & World Report (Dec. 18, 2015), *available at* http://www.usnews.com/news/articles/2015-12-18/obama-signs-cybersecurity-law-in-spending-package (last accessed Jan. 29, 2015); *see also* Cybersecurity Act of 2015, H.R. 2029, Div. N, 114th Cong. (2015), *available at* https://www.congress.gov/114/bills/hr2029/BILLS-114hr2029enr.pdf (to be included in forthcoming P.L. 114-113). Watch for a forthcoming alert with more details on this topic in the near future.

[14] *See* Office of Management and Budget, Improving Cybersecurity Protections in Federal Acquisitions Public Comment Space, *available at* https://policy.cio.gov/ (last accessed Jan. 11, 2015).

[15] *See* NIST Computer Security Division, Computer Security Resource Center, *FISMA Detailed Overview* (Apr. 1, 2014), *available at* http://csrc.nist.gov/groups/SMA/fisma/overview.html; *see also* 44 U.S.C. § 3541 *et seq.*

[16] *Id.*

[17] *See* DoD, *Defense Federal Acquisition Regulation Supplement: Network Penetration Reporting and Contracting for Cloud Services (DFARS Case 2013-D018) Interim Rule*, 80 Fed. Reg. 51739 (Aug. 26, 2015), *available at* https://federalregister.gov/a/2015-26887 (last accessed Jan. 11, 2015).

[18] *See* Council of Defense and Space Industry Associations, Comments on DFARS Case 2013-D018 "Network Penetration Reporting and Contracting for Cloud Services (Nov. 17, 2015), *available at* http://www.itic.org/dotAsset/4/2/420da80b-931b-425e-ac61-f19b57571208.pdf.

[19] DoD, *Defense Federal Acquisition Regulation Supplement: Network Penetration Reporting and Contracting for Cloud Services (DFARS Case 2013-D018) Interim Rule*, 80 Fed. Reg. 81472 (Dec. 30, 2015), *available at* https://www.federalregister.gov/articles/2015/12/30/2015-32869/defense-federal-acquisition-regulation-supplement-network-penetration-reporting-and-contracting-for.

[20] *Id.*

[21] *See, e.g.,* ISL 2013-05 (Applicability of National Industrial Security Program Operating Manual (NISPOM) Paragraph 1-301 Reporting Requirements to Cyber Intrusions (July 2, 2013).

[22] *See* Defense Information Systems Agency, United States Cyber Command (USCYBERCOM) Omnibus Contract Solicitation No. HC1028-15-R-0026 (Apr. 30, 2015), *available at* https://www.fbo.gov/spg/DISA/D4AD/DITCO/HC1028-15-R-0026/listing.html.

[23] *See* Modification No. 0002 to United States Cyber Command (USCYBERCOM) Omnibus Contract Solicitation No. HC1028-15-R-0026 (May 21, 2015), *available at* https://www.fbo.gov/spg/DISA/D4AD/DITCO/HC1028-15-R-0026/listing.html.

[24] *See* Department of the Air Force, Insider Threat Program Solicitation No. FA7014-15-R-5015 (Aug. 11, 2015), *available at* https://www.fbo.gov/spg/USAF/AFDW/11CONS/FA7014-15-R-5015/listing.html.

[25] *See* OMB, Memorandum for Chief Information Officers, *Security Authorization of Information Systems in Cloud Computing Environments* (Dec. 8, 2011), *available at* https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fedrampmemo.pdf.

[26] *See* GSA, FedRAMP Program Overview, *available at* https://www.fedramp.gov/about-us/about/ (last accessed Jan. 11, 2015).

[27] *Id.*

[28] *See* GSA FedRAMP, About FedRAMP, *available at* http://www.gsa.gov/portal/category/102375 (last accessed Jan. 11, 2015).

[29] *Id.*

[30] *Id.*

[31] *See* GSA FedRAMP, Cloud Services Providers, *available at* http://www.fedramp.gov/participate/csps/ (last accessed Jan. 11, 2015).

Pillsbury Winthrop Shaw Pittman LLP is a leading international law firm with 18 offices around the world and a particular focus on the energy & natural resources, financial services, real estate & construction, and technology sectors. Recognized by *Financial Times* as one of the most innovative law firms, Pillsbury and its lawyers are highly regarded for their forward-thinking approach, their enthusiasm for collaborating across disciplines and their unsurpassed commercial awareness.