BRIEFING PAPERS® SECOND SERIES

WEST®

PRACTICAL TIGHT-KNIT BRIEFINGS INCLUDING ACTION GUIDELINES ON GOVERNMENT CONTRACT TOPICS

CYBERSECURITY FOR GOVERNMENT CONTRACTORS

By Robert Nichols, Susan Booth Cassidy, Anuj Vohra, Kayleigh Scalzo, and Catlin Meade

President Obama has identified "cyber threats" as "one of the gravest national security dangers that the United States faces."[1] Indeed, U.S. federal agency computer systems are subject to billions of cyber attacks every month.[2] The U.S. Government does not publish statistics regarding cyber attacks on its contractors. But without a doubt, contractors face a similar proliferation of attempted breaches to their information systems.

The U.S. Government and its contractors are frequent cyber targets in part because the Government "is the largest single producer, collector, consumer, and disseminator of information in the United States and perhaps the world."[3] This repository of information includes highly classified national security secrets, details on the operations and security systems of the nation's critical infrastructure, public- and private-sector intellectual property, and the personal information of private individuals. Such data are often stored on or flow through contractor systems, which increasingly are tied to Government information technology (IT) networks. The Legislative and Executive Branches have responded by issuing various laws, regulations, policies, and guidance that apply to federal agencies and, increasingly, to contractors.

IN BRIEF

Overview Of The Cybersecurity Threat

Statutory & Regulatory Requirements
- Federal Information Security Management Act
- Contractor Information Safeguarding Rules
- Maintaining Supply Chain Integrity Rules

Cybersecurity Executive Order
- E.O. 13626 Mandates
- GSA & DOD Working Group Report
- Agency Information Sharing Programs

NIST Cybersecurity Framework
- Framework's Structure
- Framework Core
- Framework Implementation Tiers
- Framework Profile
- Using The Framework
- Next Steps For The Framework
- Framework's Impact On Government Contractors
- Framework As A Potential Standard Of Care

Legal Risks To Government Contractors
- Impact Of Cybersecurity Requirements On Traditional Government Contractor Risks
- Flowing Down Cybersecurity Requirements
- Indemnification & Damages Provisions In Prime Contracts
- Cybersecurity Compliance: Reporting Obligations & Government Audits
- Costs Of Cybersecurity

Risk Mitigation & Potential Defenses To Cybersecurity Liability
- Insurance
- SAFETY Act
- Government Contractor Defense & Theories Of Immunity
- Public Law No. 85-804 Indemnification

Conclusion

The authors are attorneys in Covington & Burling LLP's Government Contracts practice group in Washington, D.C. They work collaboratively with the firm's other key practice groups to advise and represent clients on Government and commercial cybersecurity requirements, standards for safeguarding Government and other client information, cyber insurance and other risk-shifting mechanisms, the conduct of investigations and responses to cyber breaches, and the defense against the lawsuits and other legal consequences of cyber incidents. Robert Nichols is a partner and co-chair of the Government Contracts practice group. Susan Cassidy is also a partner in the practice group and, prior to joining Covington, was in-house counsel for a large defense and aerospace contractor supporting both intelligence and defense programs. Anuj Vohra is an associate in the practice group, having previously served as a Trial Attorney in the Department of Justice's Commercial Litigation Branch. Kayleigh Scalzo is an associate in the Government Contracts and Litigation practice groups and was previously a law clerk for The Honorable Bruce M. Selya of the U.S. Court of Appeals for the First Circuit. Catlin Meade is an associate in the Government Contracts practice group who focuses on internal investigations, cybersecurity policy and compliance, and the SAFETY Act.

This Briefing Paper presents a comprehensive summary of the key legal issues and evolving compliance obligations that contractors now face in the federal cybersecurity landscape. It begins with an overview of the most prevalent types of cyber attacks and targets, as well as the federal cybersecurity budget. Next, the Paper outlines the current federal cybersecurity legal requirements applicable to Government contractors, including statutory and regulatory requirements, the President's 2013 cybersecurity Executive Order (E.O.), and the resulting "cybersecurity framework" issued by the National Institute of Standards and Technology (NIST) in February 2014, as well as highlights further developments expected this year. Finally, it identifies and discusses the real-world legal risks that contractors face when confronting cyber attacks and addresses the availability of possible liability backstops in the face of such attacks.[4]

Overview Of The Cybersecurity Threat

There is no unified, controlling definition of cybersecurity, but "measures intended to protect information systems—including technology (such as devices, networks, and software), information, and associated personnel—from various forms of attack"[5] provides a good working definition. Cybersecurity threats arise from a variety of actors and for a variety of purposes, including criminals seeking financial gain through the theft of proprietary information; hackers pursuing a range of social, political and other agendas; insiders seeking to cause harm or embarrassment to their employers; terrorists seeking to damage U.S. national security; and nation states (and their agents) conducting military operations, economic espionage, and other activities.[6] Attacks may target the U.S. military, critical infrastructure,[7] and private companies working in the defense and other critical infrastructure sectors.[8] Attackers may steal Government secrets or other sensitive Government information, intellectual property or other confidential and business proprietary information, and personal information.[9] These attacks can result in an array of financial, security, and reputational damages. Cyber attacks subject companies whose systems are breached to increasing costs stemming from competitive injuries due to stolen intellectual property, reputational damage, and investigation and remediation measures.

Federal agencies are prime targets of cyber attacks. The Office of Management and Budget (OMB) found that, on average, agencies detect only 63% of cybersecurity incidents,[10] meaning that tens of thousands of incidents go undiscovered. Similarly, the U.S. Government Accountability Office (GAO) reported in 2012 that 18 of 24 major federal agencies had inadequate security controls for financial reporting, and the Inspectors General for 22 of these agencies reported information security as a major management challenge.[11]

Cyber attacks can take several forms, including computer viruses, phishing, trojan horses, worms,[12] denials of service, back doors, rogue access points,[13] and "ransomware"—through which an attacker encrypts a victim's needed or valuable data and holds it for ransom.[14] The threat platforms for cyber attacks also are expanding as private and Government organizations increasingly integrate mobile devices into their IT networks and systems.

In light of these growing threats, cybersecurity is a clear Government priority. The President's

WEST®

BRIEFING PAPERS

Briefing Papers® (ISSN 0007-0025) is published monthly except January (two issues) and copyrighted © 2014 ■ Valerie L. Gross, Editor ■ Periodicals postage paid at St. Paul, MN ■ Published by Thomson Reuters / 610 Opperman Drive, P.O. Box 64526 / St. Paul, MN 55164-0526 ■ http://www.legalsolutions.thomsonreuters.com ■ Customer Service: (800) 328-4880 ■ Postmaster: Send address changes to Briefing Papers / PO Box 64526 / St. Paul, MN 55164-0526

proposed budget for Fiscal Year (FY) 2014 allocates over $13 billion to cybersecurity programs.[15] Much of this spending is allocated to IT staffing for security management, approximately 40% of which is currently handled by private contractors. Government spending on IT staffing alone is likely to reach $6.2 billion by 2017, with private contractors comprising 60% of that cost.[16]

Given that concerns about cybersecurity are Government-wide, responsibility for guarding against these risks does not fall neatly within the purview of a single federal agency. Without uniform policies and regulations, contractors are faced with unique and sometimes conflicting cybersecurity requirements that a variety of agencies have incorporated into their acquisition processes. Moreover, the scope of federal cybersecurity regulations is expanding, and standards that currently apply only to defense, intelligence, and critical infrastructure contractors are likely to extend to civilian agencies and may eventually serve as industry-neutral, commercial-sector standards. Because private industry owns most critical infrastructure in the United States, the private sector—both contractors and otherwise—likely will play a large part in the federal cybersecurity apparatus.

Statutory & Regulatory Requirements

■ Federal Information Security Management Act

The Federal Government has long recognized the importance of information and data security, as is demonstrated by the numerous statutes passed over the past 30 years that address, in a piecemeal fashion, different aspects of these areas.[17] Some examples include:

(1) the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984,[18] which prohibits attacks on computer systems used by the Government and in interstate and foreign commerce;

(2) the Computer Security Act of 1987,[19] which delegated to NIST responsibility for developing security standards for federal computer systems;

(3) the Paperwork Reduction Act of 1995,[20] which assigned to the OMB, through its Office of Information and Regulatory Affairs, responsibility for developing cybersecurity policies;

(4) the Clinger-Cohen Act of 1996,[21] which provided IT acquisition guidelines for federal agencies and created the role of Chief Information Officer (CIO) within individual federal agencies;

(5) the Homeland Security Act of 2002,[22] which established the Department of Homeland Security (DHS) and assigned to it, among other things, responsibilities related to cybersecurity; and

(6) the Cyber Security Research and Development Act of 2002,[23] which assigned certain cybersecurity research responsibilities to the National Science Foundation (NSF) and to NIST.

Although these laws and regulations address various aspects of cybersecurity, none provides a comprehensive framework to address the evolving and increasing threat that cyber attacks pose to Government and contractor networks.

Recognizing the need to create a framework of security controls for federal networks, Congress in 2002 passed the Federal Information Security Management Act (FISMA).[24] FISMA sought to "provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets"[25] and to ensure the "development and maintenance of minimum controls required to protect Federal information and information systems."[26] To that end, FISMA charged the Director of the OMB with "over[sight of] agency information security policies and practices," including a comprehensive list of specific responsibilities related to that oversight;[27] assigned additional cybersecurity responsibilities to NIST;[28] and required the creation of a "Federal Information Security Incident Center" to provide, among other things, information about current and potential information security threats and vulnerabilities and assist agencies in the event of a cybersecurity incident.[29]

FISMA also imposed cybersecurity responsibilities on individual federal agencies, directing

that "[t]he head of each agency shall" (1) be responsible for providing security protections that are sufficient to address the harm determined to result from a potential cyber event and for general FISMA compliance; (2) ensure that senior agency officials take sufficient measures to protect information assets in their control; (3) ensure that agency "strategic and operational planning processes" include "information security management processes"; and (4) delegate authority to the agency's CIO to ensure FISMA compliance.[30] Moreover, FISMA requires that agencies "develop, document, and implement an agency-wide information security program" that provides "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."[31] Such information security systems must be approved by the Director of the OMB and include "policies and procedures" that are compliant with both those issued by the OMB and in conjunction with NIST.[32]

FISMA's compliance requirements clarify that agencies also are responsible for the protection of "information systems used or operated…by a contractor of an agency or other organization on behalf of an agency."[33] Thus, agencies may "flow down" FISMA's requirements to contractors with control of agency information systems. Often, however, those flowdown requirements are broadly drafted, requiring the contractor to determine the appropriate means for FISMA compliance.

Federal agencies have struggled to implement FISMA's requirements. In September 2013, the GAO issued a report on the FISMA compliance efforts of 24 major federal agencies, and the effectiveness of their information security policies and practices.[34] That report concluded that, although those agencies generally had made progress in their FISMA-implementation efforts, the weaknesses in their information security programs indicated that "information security continues to be a major challenge for federal agencies."[35] The report further observed that, "[u]ntil steps are taken to address these persistent challenges, overall progress in improving the nation's cybersecurity posture is likely to remain limited."[36]

■ Contractor Information Safeguarding Rules

(1) *DFARS Rule on Safeguarding DOD Unclassified Controlled Technical Information*—In June 2011, the Department of Defense (DOD), the National Aeronautics and Space Administration (NASA) and the General Services Administration (GSA) issued a proposed rule for safeguarding unclassified DOD information.[37] In the absence of a final rule, in October 2013, Secretary of Defense Chuck Hagel issued a memorandum setting forth a number of required actions for the DOD to ensure the protection of unclassified controlled technical information (UCTI) against "cyber intrusions."[38] In November 2013, the DOD issued a final rule amending the Defense Federal Acquisition Regulation Supplement (DFARS) to add coverage regarding the safeguarding of UCTI and the reporting of cybersecurity incidents.[39] The UCTI rule defines "controlled technical information" as "technical information with military and space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination."[40]

The DFARS UCTI rule represents the most concrete impact to date on contractors trying to navigate and comply with the Government's cybersecurity requirements. A new clause included in the UCTI rule, "Safeguarding of Unclassified Controlled Technical Information," requires contractors to (1) provide "adequate security" to safeguard UCTI that is "resident on or transiting through the Contractor's unclassified information systems"; (2) timely report cybersecurity incidents and UCTI compromises to the DOD; and (3) assist the DOD with damage assessments of cybersecurity incidents.[41] This clause must be included in all new DOD solicitations and contracts, including for the acquisition of commercial items.[42] The reach of the UCTI rule does not appear limited to contract-specific UCTI; once a contractor is awarded a contract or subcontract that includes the UCTI clause, the rule presumably applies to all UCTI on the contractor's unclassified information systems.[43]

The UCTI rule defines "adequate security" for safeguarding UCTI as "protective measures that are commensurate with the consequences

and probability of loss, misuse, or unauthorized access to, or modification of information."[44] This includes, at a minimum, meeting 51 specified security controls from NIST Special Publication (SP) 800-53 covering 14 different areas of information security.[45] If a contractor fails to implement one or more of the specified controls, it must provide the Contracting Officer with a written explanation of why the control is not required or propose an alternative control or protective measure that achieves equivalent protection.[46] In addition, if a contractor determines that additional controls beyond those identified in the UCTI rule are necessary to provide adequate security, the contractor must apply those other security measures as well.[47]

In addition to the system of controls described above, the UCTI rule requires contractors to report cyber incidents that affect UCTI,[48] preserve images of affected information systems,[49] and assist the DOD in assessing any damage resulting therefrom.[50] Within 72 hours of identifying a cyber incident affecting UCTI, contractors must report certain specific information to the DOD,[51] which may pose significant challenges to Government contractors even as to determining whether their systems have been compromised. A contractor is also obligated to share files that are compromised unless it is legally prohibited from doing so.[52] Finally, following a cyber incident, contractors must review their unclassified information systems to identify further evidence of compromise, including a specific identification of any impacted UCTI.[53] Contractors must also preserve affected information for 90 days to accommodate a potential request by the DOD to review that information.[54]

The substance of the UCTI rule must be flowed down to subcontractors,[55] and prime contractors are responsible for ensuring that all cyber incidents occurring on either their own or their subcontractors' unclassified information systems are reported to the DOD. Although the rule does not impose specific penalties for noncompliance, contractors that fail to meet its requirements could be found in breach of their contracts, with all the attendant negative consequences that result from such a breach, including but not limited to termination for default, adverse past performance ratings, reduced award fees, and/or a finding that they represent a supply chain risk.

(2) *Proposed FAR Rule on Basic Safeguarding of Contractor Information Systems*—In August 2012, prior to the issuance of the final DFARS UCTI rule, the Federal Acquisition Regulation (FAR) Council proposed a broader rule that would have applied Government-wide to address basic requirements for safeguarding contractor information systems.[56] If implemented, the proposed FAR rule would apply to all solicitations and contracts where a contractor's information systems may contain nonpublic Government information[57] and would include, among others, the following controls:

(a) prohibiting contractors from processing nonpublic Government information on publicly available computers and from posting such information on publicly available webpages;

(b) requiring contractors to overwrite media used to process such information before external release or disposal; to encrypt organizational wireless networks and document files; to limit transfer of nonpublic Government information only to subcontractors with a need to know; to report loss or unauthorized disclosure of nonpublic Government information; and to exercise care when transmitting such information via voice or fax; and

(c) requiring contractors to maintain at least one physical or electronic barrier (e.g., locked room or log-on procedure) between nonpublic Government information and the public; to protect against network intrusion and data exfiltration; and to encrypt all controlled unclassified information on mobile computing devices.[58]

Perhaps most significantly, the proposed FAR rule would require that electronic transmissions containing nonpublic Government information use "technology and processes that provide the best level of security and privacy available"[59]—but without defining that standard. Contractors would be obligated to obtain a commitment from their subcontractors and external IT providers to protect unclassified DOD information with "at

least the same level of security" required by the proposed FAR rule."[60]

If implemented, the proposed FAR rule would present new compliance issues for contractors. Although its requirements are more basic than the DFARS UCTI rule, the requirement of "best level of security and privacy available, given facilities, conditions, and environment" suggests an evolving standard, as levels of available security and privacy are ever-changing. Beyond the unclear standards, compliance with the proposed FAR rule also would be difficult because the requirements deal largely with human behavior, such as maintaining physical barriers and refraining from using public computers, as opposed to implementing technological safeguards. A final rule is expected in 2014.

■ Maintaining Supply Chain Integrity Rules

(a) *Enhanced Procurement Authority for the DOD, the DOE, and the IC*—Although unable to pass comprehensive cybersecurity legislation, Congress has recognized that the supply chain for IT systems and networks is particularly vulnerable to cyber attack. Accordingly, it has granted the DOD, the Department of Energy (DOE), and agencies within the Intelligence Community (IC)[61] the "enhanced authority" to exclude a contractor from procurements for national security systems upon a determination that the contractor represents a supply chain risk.[62] For these purposes, "supply chain risk" is defined as "the risk that an adversary may sabotage, maliciously introduce unwanted functions, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of the system."[63] This enhanced authority allows these agencies to employ three different supply chain–risk management methods:

(1) exclude a source that fails to meet qualification standards for the purpose of reducing supply chain risk in the acquisition of covered systems;

(2) exclude a source that fails to achieve an acceptable rating for supply chain risk in the evaluation of proposals for contracts or a task or delivery order; and

(3) 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.[64]

There are slight differences among the grants of enhanced authority to the DOD, the DOE, and the IC. Although all three grants apply to solicitations and contracts for procurements of IT items for inclusion in a national security systems, the DOE's authority also extends to certain solicitations and contracts related to nuclear weapons and nonproliferation and counter-proliferation programs and systems.[65] The decisions to exercise this enhanced authority come from high levels within each agency and require notification to relevant congressional committees.[66]

These grants of enhanced authority raise several concerns. First, they permit the identified agencies to limit the disclosure of information about the exercise of that authority,[67] thus potentially inhibiting a company adversely affected by that exercise from challenging it. Second, the exercise of that enhanced authority is likely not reviewable in a bid protest.[68] Moreover, because agencies are encouraged to notify other agencies of perceived risks associated with particular contactors, this raises the possibility of *de facto* debarment, as other agencies follow suit after a contractor is identified as a supply chain risk. Finally, there are questions about what information an agency may rely on in making a supply chain risk determination. For example, it is unclear whether multiple reports of a cybersecurity incident under the new DFARS UCTI rule would permit the DOD, the DOE, or the IC to determine that a company poses a supply chain risk.[69]

This enhanced authority also may spur new considerations in teaming choices and proposal/bid submissions. Companies that contract with the DOD, the DOE, or the IC will need to select their lower tier contractors and teaming partners with great care to avoid companies that have been (if identifiable) or are likely to be considered a supply chain risk. One partner's designation as a supply chain risk could result in difficulties for

the other contractors in the teaming arrangement. Similarly, the exclusion of a lower tier subcontractor could lead to increased costs and other issues if the prime contractor is forced to find a replacement. Prime contractors should consider seeking certifications from subcontractors that, to their knowledge, they have not been excluded from participation in any relevant procurement involving the DOD, the DOE, or the IC.

(b) *Department of Justice, Department of Commerce, NSF, and NASA*—The Consolidated Appropriations Act of 2014 included a supply chain provision prohibiting the Department of Justice, Department of Commerce, the NSF, and NASA from acquiring "high-impact"[70] or "moderate-impact"[71] information systems where the Government has determined that there is "any risk associated with such system being produced, manufactured, or assembled by one or more entities identified by the United States Government as posing a cyber threat, including but not limited to, those that may be owned, directed, or subsidized by the People's Republic of China."[72] Once those assessments are complete, the agency head must (1) develop a mitigation strategy for any identified risks in consultation with NIST; (2) determine whether the acquisition of the information system is "in the national interest"; and (3) report that determination to the Committees on Appropriation of the House of Representatives and the Senate.[73]

These new acquisition standards create several potential procurement issues with respect to the four affected agencies. First, because the additional language is broad and lacks accompanying definitions, it is uncertain how agencies will implement the new acquisition standards. Of particular concern is the absence of any guidance for determining whether an entity presents a cyber threat or what constitutes "the national interest." Second, Contracting Officers may be less willing to procure high- or moderate-impact information systems from companies proposing products that originate in China or other perceived high-risk countries to avoid the necessary determination that the acquisition is "in the national interest" and/or reporting that determination to Congress. Finally, the Act complicates matters for contractors because it applies to only the four agencies, and each may implement the new acquisition standards differently. Thus, the new acquisition standards create yet another set of supply chain obligations that can vary by agency and contract.

(c) *DOD Counterfeit Prevention Policy and Final DFARS Rule for Electronic Parts*—The Government's concerns with supply chain risks also resulted in special provision in the National Defense Authorization Acts (NDAAs) for FY 2012 (§ 818) and FY 2013 (§ 833) addressing counterfeit parts. Section 818 requires the Secretary of Defense to assess the DOD's "acquisition policies and systems for the detection and avoidance of counterfeit electronic parts" and to update DOD policies for addressing these risks.[74] Section 833 addresses special allowability requirements for the costs of counterfeit electronic parts and the corrective actions associated with such counterfeit electronic parts.[75] To implement this requirement, on April 26, 2013, the DOD issued an internal Counterfeit Prevention Policy that addresses the prevention and detection of counterfeit material.[76] Almost a year after it issued a proposed rule on counterfeit electronic parts,[77] the DOD issued a final rule on May 6, 2014, which incorporated comments from more than 50 respondents, as well input that the DOD received from a series of public meetings it held on the issue.[78]

The DOD Policy has three identified purposes: (1) to set standards to prevent counterfeit materials[79] from entering the DOD supply chain;[80] (2) to direct anti-counterfeit measures relating to DOD weapon and information systems acquisition and sustainment; and (3) to assign responsibilities for executing these standards and measures.[81] The DOD Policy defines "materiel" to include, among other things, "system components, subcomponents, software, information and communications technology…, [and] support equipment and systems."[82] Thus, the scope of the Policy is wider than that of FY 2012 NDAA § 818 and the DFARS rule. Among the goals of the Policy is to use a "risk-based approach" to detect and prevent the use of counterfeit goods in the DOD supply chain.[83]

The final DFARS counterfeit parts rule[84] updates the DFARS to implement FY 2012 NDAA § 818[85] and FY 2013 NDAA § 833. The final DFARS counterfeit parts rule implements § 818 in three primary ways: (1) by adding definitions to DFARS

202.101 for the terms "counterfeit electronic part," "electronic part," "obsolete electronic part," and "suspect counterfeit part";[86] (2) by presenting anti-counterfeiting requirements for contractors in new DFARS 246.870, "Contractors' counterfeit electronic part avoidance and detection systems" and a corresponding clause;[87] and (3) by adding a new cost principle at DFARS 231.205-71 making unallowable as reimbursable costs—with certain exceptions—the "costs of counterfeit electronic parts or suspect counterfeit electronic parts and the cost of rework or corrective action that may be required to remedy the use or inclusion of such parts."[88] The final DFARS counterfeit parts rule applies only to counterfeit electronic parts; it does not cover all counterfeit material or items.[89]

Under the final DFARS counterfeit parts rule, contractors must "establish and maintain an acceptable counterfeit electronic part detection and avoidance system."[90] Among the 12 requirements for an "acceptable" system are risk-based processes to inspect and test electronic parts, the use of authorized suppliers, methodologies for tracing the parts of suppliers, reporting and quarantining counterfeit and suspect counterfeit electronic parts, and controlling obsolete electronic parts.[91] If a contractor fails to meet these system minima, its purchasing system may be disapproved and/or payments may be withheld.[92]

The final DFARS counterfeit parts rule applies to contractors subject to the Cost Accounting Standards (CAS),[93] as well as to all subcontractors to CAS-covered prime contractors, regardless of the subcontractors' CAS or size status.[94] Additionally, the final DFARS counterfeit parts rule applies to commercial items and commercial-off-the-shelf (COTS) items when subcontracted by a CAS-covered contractor.[95] Therefore, small business concerns, including commercial item suppliers, may be impacted if they fall within the supply chain of prime contractors subject to the CAS and thus also subject to the rule.[96]

Cybersecurity Executive Order

■ E.O. 13626 Mandates

On February 12, 2013, President Obama issued Executive Order (E.O.) 13636[97] and Presidential Policy Directive (PPD) 21,[98] which directed federal agencies to undertake a broad range of tasks aimed at enhancing the security and resilience of the nation's critical infrastructure. E.O. 13636 and PPD 21 set out an ambitious schedule of deliverables, including:

(a) directing NIST to establish a technology-neutral, voluntary cybersecurity framework;[99]

(b) promoting and incentivizing the adoption of cybersecurity practices;[100]

(c) increasing the volume, timeliness, and quality of cyber-threat information sharing;[101]

(d) incorporating cybersecurity requirements into the federal acquisition process;[102]

(e) identifying baseline data and systems requirements to enable the efficient exchange of information and intelligence relevant to strengthening the security and resilience of critical infrastructure;[103]

(f) developing a near real-time awareness capability for both physical and cyber aspects of infrastructure functions;[104] and

(g) analyzing the existing public-private partnership model and recommending options for improving the effectiveness of such partnerships in both the physical and cyber space.[105]

Over the past 15 months, federal agencies have taken strides to implement these mandates.

■ GSA & DOD Working Group Report

E.O. 13636 recognized the need to integrate cybersecurity protections through the federal acquisition process. To that end, § 8(e) of E.O. 13636 tasked agencies with harmonizing existing cybersecurity procurement requirements[106] and directed the GSA and the DOD to prepare recommendations for the President on the "feasibility, security benefits, and relative merits of incorporating security standards into acquisition planning and contract administration."[107] In response, the GSA and the DOD released a Joint Report on January 23, 2014, entitled *Improving Cybersecurity and Resilience Through Acquisition*.[108]

The Joint Report contains six recommendations aimed at "strengthening the cyber resilience of the Federal government by improving management of the people, processes, and technology affected by the Federal Acquisition System."[109] Specifically, it recommends the following Government actions:

(1) instituting baseline cybersecurity requirements as a condition for certain contract awards;[110]

(2) training the relevant Government workforce in new cybersecurity acquisition practices;[111]

(3) developing common cybersecurity definitions and increased clarity of key cybersecurity terms;[112]

(4) creating a Government-wide cybersecurity risk management strategy that identifies a "hierarchy of cyber risk criticality for acquisitions" to permit the Government to identify acquisitions that present the greatest cyber risk;[113]

(5) requiring the Government to procure certain items solely from original equipment manufacturers, authorized resellers, or other trusted sources;[114] and

(6) increasing Government accountability by holding key decisionmakers accountable for "decisions regarding the threats, vulnerabilities, likelihood, and consequences of cybersecurity risks."[115]

The Joint Report presents a starting point for the Government to incorporate cybersecurity measures into its acquisition systems and procedures. As discussed below, however, several of the Joint Report's recommendations already had been contemplated—and some portions implemented—through Executive Orders, rulemakings, internal policies and directives, and legislation. Although the Joint Report acknowledges this fact, it provides no guidance on how to align and harmonize its recommendations with other ongoing cybersecurity efforts.[116]

On March 12, 2014, the GSA issued a request for comments on its draft implementation plan for the Joint Report's fourth recommendation, the creation of a Government-wide risk management framework.[117] With this recommendation, the GSA recognized that different assets purchased by the Government present varying levels of cyber risk.[118] Therefore, "[t]he goal of this recommendation is to develop a repeatable, scalable process for addressing cyber risk in federal acquisitions based on the risk inherent to the product or service being purchased, that is flexible enough to be adapted to the various risk tolerances of end users or risk owners."[119]

The draft implementation plan appears to envision the following process: (1) creating categories encompassing similar items purchased by the Government; (2) determining which categories present a cyber risk; (3) prioritizing those categories based on their perceived cyber risk; and (4) applying overlays to each category, which will provide a specific set of minimum security controls applicable to the acquisition of items within each category.[120] The GSA has requested stakeholder input as to the feasibility of this implementation plan.[121] Presumably, the GSA will seek additional comments for the remaining recommendations.

■ Agency Information Sharing Programs

For several years, the DOD has operated the voluntary Defense Industrial Base (DIB) Cyber Security and Information Assurance (CS/IA) program,[122] in which DOD shares unclassified cyber threat information with participating DOD contractors.[123] Those DIB participants may use that information at their discretion to update their cybersecurity systems.[124] In certain circumstances, the Government will share threat information with DIB participants' Commercial Service Providers (CSPs).[125] The scope and content of the information-sharing between DOD and DIB participants is defined in formal, individualized "Framework Agreements."[126]

Similarly, the DHS operates its "Enhanced Cybersecurity Services" (ECS) program to share cybersecurity threats information with all critical infrastructure sectors, not just companies that contract with the DOD.[127] E.O. 13636 directed the DHS to expand the ECS program to promote the "policy of the United States Government to

increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities so that these entities may better protect and defend themselves against cyber threats."[128] The ECS program "does not replace an entit[y]'s existing cybersecurity capabilities"; instead, it offers "an enhanced approach" to cybersecurity providers that protect critical infrastructure entities.[129] Through the program, the DHS "works with cybersecurity organizations from across the federal government to gain access to a broad range of sensitive and classified cyber threat information," and based upon this information, develops threat "indicators" which it then shares with qualified CSPs.[130] Those CSPs can then utilize that information "to better protect their customers who are critical infrastructure entities."[131] Unlike the DOD under the CS/IA program, the DHS does not share classified cyber threat information with critical infrastructure companies other than CSPs. Despite that limitation, the expanded ECS program is an important information-sharing initiative to assist the private sector in combating ever-evolving cybersecurity threats.

NIST Cybersecurity Framework

E.O. 13636 called for NIST to establish voluntary standards for assessing cyber risks to the nation's critical infrastructure. Following a year-long drafting process, on February 12, 2014, NIST released its *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.0.[132] The Framework focuses on the critical infrastructure sectors[133] and "provides guidance to organization[s] on managing cybersecurity risk"[134] by "assembling standards, guidelines, and practices"[135] based upon previously identified effective industry approaches. In short, the Framework serves as a voluntary tool that organizations can use to strengthen their current risk management systems for the purposes of "identifying, assessing, and responding" to cybersecurity threats.[136]

■ Framework's Structure

The NIST Framework contains three component parts. The first, the Framework Core, identifies high-level activities and desired outcomes that are common across all critical infrastructure sectors. The second, the Framework Implementation Tiers, describes various approaches, from least to most comprehensive, that an organization can take to manage its cyber risk. The third, the Framework Profile, provides an organization-specific overview that incorporates components of the Framework to allow an organization to conduct a self-assessment of its current risk management processes and, as necessary, a plan for improving them.

■ Framework Core

The Framework Core begins by identifying a baseline of five high-level "functions" that organizations should be able to perform. These five essential functions are (1) *identify* potential cybersecurity risks and how to manage them; (2) *protect* the organization's ability to deliver critical infrastructure services so as to limit the impact of a potential cybersecurity event via the "implement[ation of] appropriate safeguards"; (3) *detect* cybersecurity events quickly to allow for a timely response; (4) *respond* to cybersecurity events in a manner that limits their impact; and (5) *recover* from cybersecurity events and efficiently restore impacted capabilities and services.[137]

These functions are not intended to be performed *seriatim*, but instead should "be performed concurrently and continuously to form an operational culture that addresses the dynamic cybersecurity risk."[138] To facilitate their implementation, the Framework Core also identifies corresponding categories and subcategories to which the functions relate (e.g., Asset Management, Risk Management, Access Control, Data Security), as well a nonexhaustive list of industry-based informative references exemplifying best practices to reach the desired outcome for each function.[139]

■ Framework Implementation Tiers

The Framework Implementation Tiers provide four categories for assessing the extent to which cybersecurity risk management is informed by and integrated into an organization's overall risk management practices.[140] Each Tier is composed of three parts—Risk Management Process,

Integrated Risk Management Program, and External Participation—that reflect organizational risk management structures ranging from informal and reactive, to fully developed and adaptive to constantly evolving cybersecurity threats. The Framework identifies the Tiers as follows:

(a) Tier 1, "Partial," describes an organizational structure that lacks formal cybersecurity risk management processes such that responses to cybersecurity threats are "ad-hoc" and reactive and for which there is no organization-wide approach to managing cybersecurity risk or sharing relevant cybersecurity-related information either internally or externally.[141]

(b) Tier 2, "Risk Informed," describes an organizational structure in which cybersecurity risk management processes are approved by management, though not yet established as an organization-wide policy.[142] Cybersecurity information is shared within an organization informally, and the organization lacks formal processes for sharing information externally.[143]

(c) Tier 3, "Repeatable," describes an organizational structure in which risk management systems are formally approved and expressed as policy, and in which cybersecurity practices are updated based upon mission requirements and evolving threats.[144] Similarly, there are defined organization-wide processes for managing cybersecurity risk, methods for responding to changes in risk, and information-sharing systems to allow for collaboration and risk based management decisions in the face of a cybersecurity event.[145]

(d) Tier 4, "Adaptive," describes an organizational structure that is continually being updated to incorporate lessons learned from prior events, as well as indicators of ever-changing future cybersecurity threats.[146] In such a system, cybersecurity risk management is "part of the organizational culture," and internal and external information-sharing systems are defined and robust.[147]

In light of the Framework's voluntary nature, NIST does not suggest that the Framework's successful implementation requires an organization's cybersecurity protections to fall within a specific tier. Rather, NIST encourages organizations to use the Framework as a guide to achieve their own desired outcomes based on their self-determined "Target Profile" (discussed below).[148] The Framework encourages organizations to move to Tier 2 or greater, but only "when such a change would reduce cybersecurity risk and be cost effective."[149] Nonetheless, a reasonable reading of the Framework suggests that an organization involved in critical infrastructure is better served with risk management processes that are closer to Tier 4 than to Tier 1.

■ Framework Profile

After organizations identify their core functions and implementation Tiers, the Framework directs them to develop a Profile that combines the Framework's identified core functions and their own needs, resources, and risk tolerances to create a "roadmap for reducing cybersecurity risk."[150] A Profile serves as an organization's self-assessment of its cybersecurity risk management processes weighed against "organizational and sector goals,...legal/regulatory requirements and industry best practices, and . . . risk management priorities."[151] The Framework does not provide a template for an organizational Profile, instead "allowing for flexibility in implementation."[152]

The Framework contemplates that each organization create two separate Profiles. The first, a "Current Profile," identifies an organization's current state of cybersecurity readiness and outcomes presently achieved.[153] The second, a "Target Profile," identifies an organization's desired but unachieved cybersecurity outcomes.[154] By comparing the two, organizations can pinpoint gaps in their existing cybersecurity posture, develop an action plan to address them, and reduce their overall cybersecurity risk.[155]

■ Using The Framework

The NIST Framework emphasizes that it is voluntary and intended to complement, not

replace, an organization's existing business and cybersecurity operations.[156] Accordingly, it eschews a "one-size-fits-all approach to managing cybersecurity risk"[157] and permits organizations to apply the Framework to fit their specific needs.[158] The Framework also recommends that companies consider incorporating into their cybersecurity programs privacy principles such as data minimization, transparency and use limitations, and accountability and auditing. To this end, NIST plans to host a privacy workshop and develop more specific privacy technical standards and best practices to be incorporated into the Framework.[159]

Finally, and as discussed in more detail below, although the Framework repeatedly emphasizes its voluntary nature, organizations—especially those within the 16 identified critical infrastructure sectors—should be aware that sector-specific agencies may look to the Framework in exercising their existing regulatory authority, and eventually courts or other regulators may come to regard the Framework as establishing a set of reasonable practices against which liability could be judged. Moreover, as is explained in more detail below, that possibility—that the Framework could be used to determine a reasonable standard of care as relates to cybersecurity protections—suggests that all companies, not just those in critical-infrastructure sectors, should consider using the Framework as a tool to assess the adequacy of their cybersecurity protections.

■ Next Steps For The Framework

NIST characterizes the Framework as "a living document" "to be updated and improved as industry provides feedback on implementation."[160] Consistent with that approach, on the same day that it released Version 1.0 of the Framework, NIST also released a "Roadmap for Improving Critical Infrastructure Cybersecurity."[161] The Roadmap "discusses NIST's next steps with the Framework and identifies key areas of development, alignment, and collaboration."[162] In particular, the Roadmap highlights "[s]everal high-priority areas for development, alignment, and collaboration," which were selected "based on stakeholder input."[163] Those areas of development include, among other things, addressing the shortage of skilled cybersecurity workers; aligning and developing cybersecurity policies across federal agencies; promoting supply-chain risk management; and revisiting the privacy concerns associated with cybersecurity vigilance.[164] The Roadmap also indicates that, "[i]n the interest of continuous improvement," NIST will keep accepting public comments about the Framework until it provides formal notice of revision to Version 1.0.[165]

■ Framework's Impact On Government Contractors

Given the voluntary nature of the NIST Framework and that it was only recently released, the Framework's impact upon entities contracting with the Federal Government is unclear. Nevertheless, in the absence of legislation or regulations imposing uniform cybersecurity requirements on Government contractors, the Framework may provide a starting point for contracting agencies to impose some basic standards in their contracts. Indeed, the November 2013 DOD and GSA Joint Report (discussed above) specifically recommended the creation, where appropriate, of "baseline cybersecurity requirements as a condition of contract award."[166] Elements of the Framework could be used to establish such a baseline.

The Framework itself appears to contemplate this possibility. In its "How to Use" section (under the subheading "Communicating Cybersecurity Requirements with Stakeholders"), the Framework states that "[a]n organization may utilize a Target Profile to express cybersecurity risk management requirements to an external service provider (*e.g.*, a cloud provider to which it is exporting data)."[167] It further states that a "critical infrastructure sector may establish a Target Profile that can be used among its constituents as an initial baseline Profile to build their tailored Target Profiles."[168] Thus, although, taken as a whole, the Framework is too broad and open-ended to serve as a baseline set of cybersecurity controls, procuring agencies could include Target Profiles among a solicitation's "Special Contract Requirements." Such a special requirement could mandate, for example, that a contractor have cybersecurity risk management systems that demonstrate particular

desired outcomes or that are appropriate for a Tier 4 Adaptive organizational structure.

■ Framework As A Potential Standard Of Care

Although the NIST Framework is voluntary, corporate leaders and directors should not disregard it as a mere aspirational ideal. The Framework is intended to assist senior executives and business leaders in understanding cybersecurity risk and deciding on best practices to guard against such risk,[169] and it would not be unexpected for companies to seek to require business partners to comply with the Framework. Similarly, there is the possibility that plaintiffs' counsel may try to hold out the Framework as a proposed standard of care in future litigation. Corporate leaders, therefore, should be aware of this risk and make informed, proactive decisions about the current status and possible future of their cybersecurity programs.

It remains unclear whether plaintiffs' counsel could successfully argue in a negligence suit that the Framework constitutes a standard of care against which a company's actions should be judged. In a typical common-law context, the standard of care is determined by asking what a hypothetical reasonable and prudent person would do in the same circumstance.[170] A common-law standard of care must have some acceptance in the community, as a reasonable and prudent person would not abide by an obscure standard that an ordinary actor would not realistically consider following.[171] In that sense, the Framework's potential transformation into a standard of care could be a self-fulfilling prophecy: if companies are concerned about the possibility of liability resulting from noncompliance with the Framework, either contractually or through tort suits, they may scramble to comply with it, thereby potentially creating the objective consensus necessary for courts to find that a standard of care exists. The facts that industry participants were intimately involved in the creation of the Framework and that the Framework is intended to reflect already existing consensus standards could assist plaintiffs' counsel in forming a persuasive argument.[172]

Even if that community consensus is not realized, plaintiffs' counsel also may argue that the Framework should be equated to a statute or administrative rule.[173] Laws and rules may form the basis for standards of care owed in particular situations, at which point they supplant the ordinary common-law standard.[174] Those laws and rules may not, however, play such a role if they were not intended to protect either the general public or the group of which the plaintiff is a member, or if they were not intended to protect against the particular type of injury suffered.[175] Additionally, the law or rule in question must impose a "specific duty," sometimes defined as "a positive and definite standard of care whereby a jury may determine whether there has been a violation thereof by finding a single issue of fact."[176]

But regardless of whether the Framework could be equated to a law or rule or is poised to develop into an ordinary common-law standard of care, it seems unlikely that the Framework could be understood to impose one or more "specific duties," compliance with which would turn on discrete issues of fact. Rather, the Framework appears to function as a kind of adaptable how-to kit for companies to consider and address cybersecurity concerns; it does not set out specific, affirmative obligations.[177] Indeed, the Framework explicitly indicates that it does not provide "a checklist of actions to perform."[178] The DHS even has declined to define what "adoption of" or "compliance with" the Framework means, instead explaining that "[a]doption of the Cybersecurity Framework will look different for every organization," and "[t]here is no 'right' or 'complete' way to use the Framework."[179] This emphasis on flexibility, extensibility, and customizability undercuts the Framework's repurposing as a standard of care.[180]

Nevertheless, the Framework highlights the duty of companies to be vigilant about cybersecurity. It emphasizes that cybersecurity risk is "[s]imilar to financial and reputational risk" and "affects a company's bottom line," with the potential to "drive up costs and impact revenue," as well as "harm an organization's ability to innovate and to gain and maintain customers."[181] Corporate leaders play an integral role in that vigilance,[182] and the Framework promises "a concise way for

senior executives and others to distill the fundamental concepts of cybersecurity risk so that they can assess how identified risks are managed, and how their organization stacks up at a high level against existing cybersecurity standards, guidelines, and practices."[183]

In addition to ordinary negligence suits, it is also possible that plaintiffs' counsel may seek to rely on the Framework as a basis for shareholder derivative actions against corporate boards, challenging board decisions regarding cybersecurity controls. Although, at present, it would be a stretch to portray the Framework as part of a board's fiduciary duties, this has the potential to change if the Framework becomes mandatory or develops into a standard of care. At that point, a board of directors might be at risk of breaching its fiduciary duties by failing to consider thoroughly the Framework when making decisions about cybersecurity. That risk would be even greater for a board that wholly failed to consider cybersecurity issues at all—particularly given the prevalent concern that boards are insufficiently informed about cyber vulnerabilities and the effects of potential cyber attacks.[184]

In sum, diligent corporate officers, regardless of industry or sector, should be aware of the Framework, take advantage of the continuing opportunity to influence its development, and ensure that their companies consider the NIST recommendations when evaluating cyber risks. Even beyond the context of the Framework specifically, the involvement of corporate boards and senior leaders is critical to the strength and efficacy of any cybersecurity program.[185] Cybersecurity is not a matter to be relegated to IT departments; it must be addressed at the highest levels of a company.[186]

Legal Risks To Government Contractors

Federal contractors that fail to implement adequate cybersecurity measures face greater legal risk than their commercial counterparts. These risks include a lack of and inconsistent Government rules, regulations, and standards. Although agencies such as the DOD, the GSA, and NIST have been particularly engaged on the topic, the Government lacks even a unified set of cybersecurity-related definitions. Furthermore, while some agencies address cybersecurity by assigning risks to contractors through regulations and guidance, others do so through individually negotiated contract terms. As a result, there is currently no comprehensive, considered balance of risk allocation that applies across the Government. Such a fragmented approach breeds uncertainty both as to the scope of contractor obligations and potential liability, which are likely only to expand in the near future. And as the Government's approach to cybersecurity evolves, contractors' obligations will likely only expand.

■ Impact Of Cybersecurity Requirements On Traditional Government Contractor Risks

Government contractors already face significant risks arising from performance on federal contracts. A breach of a Government contract carries with it consequences that go well beyond those available in a commercial breach of contract action that the Government is likely to rely on when confronted with contractor performance problems related to cybersecurity.

In general, noncompliance with the terms of a Government contract may result in the Government's termination of that contract for default.[187] While the loss of the contract (and associated potential reprocurement costs and other penalties that may attach) are harmful enough, federal agencies also use contractor performance to make both responsibility determinations—yes/no assessments on a contractor's capabilities, systems, and resources to perform a solicited contract[188]—and past performance evaluations, which consider a contractor's prior performance as an indicator of results on future contracts.[189] Cybersecurity requirements will only increase these risks. For example, a denial-of-services attack that interferes with a contractor's ability to meet certain service level-agreement standards may adversely impact the contractor's past performance ratings or lower its award fee score. Likewise, a cyber attack resulting in the inadvertent release of information that violates contractual information-sharing limitations could result in a show cause or cure notice. And, if a cybersecurity incident is sufficiently serious, under the Federal Government's

new enhanced procurement authority, a contractor could be excluded from a competition after being designated a supply chain risk.[190]

Companies that fail to comply with applicable cybersecurity rules or that otherwise do not take a responsible approach to cyber threats, also may face administrative suspension and debarment. Suspension and debarment are tools by which the Government protects its interests by ensuring that federal agencies do not do business with nonresponsible contractors.[191] Agencies may suspend or debar contractors for any number of reasons, including serious violations of regulations, willful failure to perform contractual obligations,[192] or "any other cause of so serious or compelling a nature that it affects the present responsibility of the contractor."[193] A suspended or debarred contractor is restricted from securing any new federal contracts as either a prime or subcontractor.[194] Suspension and debarment also have collateral impacts on business with state and local governments and in some commercial areas.[195]As such, the direct and indirect consequences of suspension and debarment may be severe, particularly for companies that regularly do business with the Government.

Finally, the False Claims Act (FCA)[196] imposes civil liability on any person who "knowingly presents, or causes to be presented, a false or fraudulent claim for payment or approval" or "knowingly makes, uses, or causes to be made or used, a false record or statement material to a false or fraudulent claim."[197] Courts have found violations of the FCA based upon an actor's "reckless disregard," defined as an "aggravated" form of gross negligence or "an extreme version of ordinary negligence."[198] In the contracting context, a contractor's noncompliance with contract requirements may rise to the level of reckless disregard under the theory of "implied certification." Under this theory, "the act of submitting a claim for reimbursement itself implies compliance with governing federal rules that are a precondition to payment," and, therefore, contract noncompliance, even where unrelated to the claim for payment, may give rise to an FCA violation.[199] In the face of heightened cybersecurity rules and regulations, contractors face the increased risk of an alleged FCA violation under an implied certification theory if they recklessly fail to implement appropriate and contractually required cybersecurity safeguards.[200]

All of the above demonstrate how new cybersecurity requirements can heighten old contracting risks.[201] Accordingly, contractors must take steps to ensure that they have a complete and thorough understanding of their contract's cybersecurity requirements, and that they have taken the appropriate steps (ideally, ones that have been approved by the Government) to comply with them.

■ Flowing Down Cybersecurity Requirements

Not only must prime contractors and subcontractors remain apprised of evolving cybersecurity standards, they must examine those evolving standards for their potential applicability to subcontracts and vendor agreements. For example, under the DFARS UCTI rule, a prime contractor must ensure that its subcontractors are providing "adequate security" to safeguard UCTI, timely reporting cybersecurity incidents and UCTI compromises, and assisting the prime contractor and DOD with damage assessments of cybersecurity incidents.[202] Furthermore, the new UCTI rule not only mandates that prime contractors flow down safeguarding and reporting requirements to their subcontractors, but also makes prime contractors responsible for reporting cybersecurity incidents on their subcontractors' networks.[203] These reporting requirements may require some contractors to modify their subcontractor and vendor agreements to meet their obligations to the Federal Government without violating restrictions imposed by vendors and suppliers as to their proprietary information.

At the same time, the NIST Framework and other Government guidance and policies may be voluntary or vague, making it difficult for a prime to determine what to flow down to lower level contractors or vendors. This problem may be exacerbated when working with suppliers that have relatively little Government business, are unfamiliar with Government flowdowns, or lack incentives to invest in Government-mandated compliance functions. Although prime contractors entering into vendor agreements may be tempted to rely on commercial contracts that flow down only mandatory Government procurement

clauses, this approach leaves them at risk when it comes to cybersecurity.

■ Indemnification & Damages Provisions In Prime Contracts

In the absence of Government-wide cybersecurity regulations, agencies are increasingly turning to unique contract clauses to address cyber risk allocation. For example, the Department of Interior recently issued a solicitation for a 10-year, $1 billion cloud computing contract that contained the following indemnification clause:[204]

> The Contractor shall hold and save the Government, its officers, agents and employees, harmless from liability of any nature or kind, including costs and expenses to which they may be subject, for or on account of any or all suits or damages of any character whatsoever resulting from injuries or damages sustained by any person or persons or property by virtue of performance of this contract, arising or resulting in whole or in part from the fault, negligence, wrongful act or wrong mission of the Contractor, or any subcontractor, or their employees, agents, etc.

The inclusion of such clauses—which may also include sweeping indemnification language and liquidated damages—can significantly increase the risks to contractors resulting from potential cybersecurity incidents. Therefore, in reviewing the risks associated with the submission of a proposal in response to a solicitation, company counsel should integrate potential cybersecurity risks into their business reviews. Whether those risks can be negotiated to allocate cyber risks more equitably should play an important role in the cost/benefit analysis of contracting with the Government.

■ Cybersecurity Compliance: Reporting Obligations & Government Audits

The cybersecurity reporting requirements contained in laws and regulations such as FISMA and the DFARS UCTI rule are not the only such obligations governing contractors. The FY 2013 NDAA contains additional cyber reporting requirements for contractors holding security clearances.[205] Agencies are also including *ad hoc* reporting requirements in their solicitations.[206] Additionally, if a contractor's information system is compromised due to a cybersecurity incident, almost every state requires the disclosure of the incident if the compromised data includes personally identifiable information.[207]

In October 2011, the Securities and Exchange Commission (SEC) published guidance on corporate disclosure requirements relating to cybersecurity, explaining that registered companies should "disclose the risk of cyber incidents if these issues are among the most significant factors that make an investment in the company speculative or risky" or "that a reasonable investor would consider important to an investment decision."[208] The SEC directs that a registered company's disclosure determination should be based upon its evaluation of all relevant information, including but not limited to prior cybersecurity incidents, their severity and frequency, the likelihood and impact of their reoccurrence, and the company's established preventative measures.[209]

In addition to imposing new reporting requirements, many of the laws, regulations, and standards described in this PAPER also allow the Government to audit and monitor contractor compliance with federal cybersecurity requirements. For example, the GSA demands broad audit rights with regard to contractor IT systems to ensure adequate cybersecurity measures in its "Security Requirements for Unclassified Information Technology Resources" contract clause:[210]

> The Contractor shall afford GSA access to the Contractor's and subcontractor's facilities, installations, operations, documentation, databases, IT systems and devices, and personnel used in performance of the contract, regardless of the location. Access shall be provided to the extent required, in GSA's judgment, to conduct an inspection, evaluation, investigation or audit, including vulnerability testing to safeguard against threats and hazards to the integrity, availability and confidentiality of GSA data or to the function of information technology systems operated on behalf of GSA, and to preserve evidence of computer crime. This information shall be available to GSA upon request.

Similarly, the Office of Personnel Management (OPM) requires contractors to grant continuous access to their systems and infrastructure through inclusion of clause 1752.239-86, "Contractor System Oversight/Compliance," in its solicitations. That clause directs that:[211]

> The contractor shall provide logical and physical access to the contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases upon request. The contractor will be expected to perform automated scans and continuous monitoring activities which may include, but not limited to [*sic*], authenticated and unauthenticated scans of networks, operating systems, applications, and databases and provide the results of the scans to OPM or allow OPM personnel to run the scans directly.

The DHS operates a program to oversee compliance with FISMA, OMB guidelines, and applicable NIST guidelines for contractors and vendors that provide services to or manage systems on behalf of a Government agency.[212] Although the new DFARS UCTI rule does not authorize new audit capabilities for the Government, in comments on the rule, the DOD recognized that audits "will be conducted at the discretion of the contracting officer in accordance with the terms of the contract."[213] And the FY 2013 NDAA authorizes the DOD to access the networks of cleared defense contractors "to conduct forensic analysis" of security functions and possible breaches.[214]

In addition, the Defense Contract Audit Agency (DCAA) functionally may monitor and audit a contractor's cybersecurity program even in the absence of a cybersecurity incident. The DCAA conducts audits for the DOD and other federal agencies as pertains to their procurement and contracting functions.[215] As part of those audits, the DCAA ensures that contractors are "establishing and maintaining adequate internal controls"—defined as "a process effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories: (a) reliability of financial reporting, (b) effectiveness and efficiency of operations, and (c) compliance with applicable laws and regulations."[216] As a result, a contractor's compliance with cybersecurity requirements and best practices—as well as the general health and strength of its cybersecurity program—may be examined in the course of a DCAA audit.

Along the same lines, the SEC has identified "Technology" as one of its most significant examination initiatives, explaining that it—[217]

> may conduct examinations on governance and supervision of information technology systems for topics such as operational capability, market access, and information security, including risks of system outages, and data integrity compromises that may adversely affect investor confidence. Among other things, the [SEC] hopes that these examinations will help the industry and the Commission to better understand operational information technology risks and potential methods to help mitigate and effectively manage those risks.

As a result of these heightened reporting and auditing requirements, companies cannot hide or downplay material cybersecurity vulnerabilities or compromises without the potential for Government objection. Thus, companies must be prepared to have their cybersecurity compliance questioned when an incident occurs and a reporting requirement makes that incident a public matter.

■ Costs Of Cybersecurity

Contractors that cultivate and maintain robust cybersecurity programs not only benefit because such programs help protect a company's data security, but because a Government buyer may value a sophisticated cybersecurity approach, resulting in a technical advantage in a competitive procurement. Those benefits notwithstanding, contractors should balance the considerable costs associated with a robust cybersecurity system against the possibility that some of those costs may not be immediately recoverable under Government contract cost principles.[218]

As an initial matter, there are significant internal costs associated with creating an effective cybersecurity program. Those costs may include, among other things, hiring personnel and implementing technology capable of the vigilance and responsiveness required by ever-evolving cyber threats. And there may be significant external costs, including engaging third-party experts and consultants to provide appropriate and tailored technology solutions, compliance policies and procedures, and assessments of contract and insurance policies, as well as "organizational changes, deploying additional personnel and protection technologies, [and] training employees."[219] During and after a cybersecurity breach, contractors are likely to incur additional costs from, among

other things, third-party claims, internal compliance enhancements, intellectual property losses, and reputational harm.[220]

Under Government contract cost accounting principles, to be recoverable, such costs must be included in the contractor's fixed-price proposal or, for cost-type contracts, charged to overhead rates. Indeed, the DFARS UCTI rule imposes significant new requirements and obligations with regard to reporting cyber incidents and assisting the DOD with damage assessments, but will only reimburse contractors for the costs of these activities as reimbursable costs under cost-reimbursement contracts.[221] This leaves commercial item contractors, such as those that provide much of the commercial IT to the Government, with no direct reimbursement of these costs. Even for those contractors that can charge these costs to the Government through their overhead rates, there is no guarantee that Government auditors would consider the costs incurred during and after a cyber incident to be reasonable under FAR Part 31.[222] While the authors are unaware of circumstances where post-breach costs have been disallowed, contractors should be prepared for the Government to consider, under FAR Part 31's "prudent person" standard, whether the contractor had adequate cybersecurity protections in place prior to the breach, using Government-provided guidance, such as the NIST Framework, as a potential baseline for that consideration.

Risk Mitigation & Potential Defenses To Cybersecurity Liability

Notwithstanding their best efforts to implement compliance programs, contractors are likely to face increasing litigation related to their cyber activities. For instance, as a result of a cyber attack on a contractor's network, a contractor's business partner may suffer intellectual property losses for data held on that network, or the attack may spread to the business partner's network through connected systems without adequate cyber protections. Such harm could result in claims based on, for example, tort, breach of contract, and/or breach of privacy data, seeking compensation for, among other things, adverse business impacts or losses of intellectual property. As with other litigation risks, the standard of care that a company takes to recognize the cyber risks and to impose sufficient internal controls to help mitigate those risks will both affect the likelihood of harm and bolster the defenses the company can raise to defend its conduct in response to litigation threats.

■ Insurance

An emerging insurance market seeks to fill in gaps in traditional policies that fail to address cyber risk. These new policies are marketed under different names such as technology coverage, privacy liability, network security liability, internet media liability, and technology stretch endorsements. The policies are not standardized, which can make it difficult to compare the offered coverage and exclusions, but they often include some combination of: network liability, electronic media liability, technology errors and omissions, business income loss, data and network restoration losses, forensic investigation expenses, crisis management, and extortion threats. These policies also often come with various limitations (such as relatively low sublimits for certain types of claims) and exclusions, which require a detailed analysis to determine the extent of coverage. The White House has said that it will collaborate with the insurance industry to create underwriting practices that increase competition in the insurance market.[223]

Additionally, contractors may seek insurance coverage against cyber attacks through a number of more-traditional policies, including:

(1) First-party property and business interruption policies, which generally pay for direct physical loss or damage to covered property (such as IT systems) and the resulting loss of business income. These policies typically exclude the loss of electronic data unless specifically included.

(2) Commercial crime and employee dishonesty policies provide coverage for computer-related theft by employees and third parties, but often exclude computer programs, electronic data, and certain financial transactions. The cyber-related coverage of these types of policies has been the subject of recent litigation.[224]

(3) Commercial general liability (CGL) policies have a broad duty to defend against third-party claims that potentially fall within the CGL coverage for violation of privacy claims. However, data breach-related exclusions are becoming more prevalent, and some courts have ruled that the standard-form CGL privacy coverage does not apply to a data breach.

(4) Directors' and officers' insurance, which may cover claims against officers and directors for failure to prevent a data breach.

Notwithstanding the potential availability of these policies, deciphering how they fit together to create sufficient insurance coverage for a range of cyber losses is a challenge facing contractors given the growing and ever-evolving cyber threat.

■ SAFETY Act

As part of the Homeland Security Act of 2002,[225] Congress enacted the Support Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act of 2002, which limits liability for sellers of qualified anti-terrorism technologies through a system of risk and litigation management.[226] The SAFETY Act is intended to incentivize potential sellers of anti-terrorism technologies to develop, deploy, and commercialize technologies that could save lives by limiting the threat of liability arising from such activities.[227] This statute may provide an additional backstop against cyber-related liabilities under some circumstances. For instance, in January 2014, the DHS awarded a SAFETY Act designation to an organization engaged in the provision of technology designed "to deter, detect, delay, defeat or respond to a physical or cyber attack against any form of chemical operation."[228]

Nevertheless, the extent to which the SAFETY Act may limit cyber-related liability is unclear. SAFETY Act certification would protect only against liability arising out of cyber incidents that occur as part of an act of terrorism, which is defined as "any act that the Secretary [of Homeland Security] determines meets the [following] requirements:" (a) "is unlawful"; (b) "causes harm to a person, property, or entity, in the United States"; and (c) "uses or attempts to use instrumentalities, weapons or other methods designed or intended to cause mass destruction, injury or other loss to citizens or institutions of the United States."[229] This definition is a narrow one in which traditional cyber attacks—which can inflict substantial harm without "mass destruction, injury or other loss to citizens or institutions of the United States"—may not fit.

Recognizing this limitation, in December 2013, a bill was introduced in the U.S. House of Representatives to expand SAFETY Act coverage to include cyber incidents.[230] As introduced, the bill defines a "qualifying cyber incident" as "any act that the Secretary determines meets the [following] requirements": (1) is unlawful or exceeds authority; (2) "disrupts or imminently jeopardizes the integrity, operation, confidentiality, or availability of" information systems; (3) gains access to a network or system resulting in misappropriation, corruption of data, operation disruption, or an adverse effect; and (4) causes harm that results in material damage or disruption "severely affecting the United States population, infrastructure, economy, [or] national morale."[231] While the bill would clearly expand the scope of the statute's protections for contractors in involved in cybersecurity, its prospects for passage are uncertain.

■ Government Contractor Defense & Theories Of Immunity

There are a handful of traditional defenses and immunities that contractors may raise in responding to tort-based, third-party claims arising out of their work for the Government: the Government contactor defense, shared sovereign immunity, and official immunity. Although these defenses and immunities are new to the cybersecurity context, they have the potential to be applied in certain cyber-related circumstances.

The Government contractor defense may protect a contractor from state law tort suits where the contractor is working at the Government's direction and state law tort liability presents a "significant conflict" with federal policy.[232] The Supreme Court first articulated this defense in *Boyle v. United Technologies Corp.*[233] *Boyle* identified two main concerns implicating the Government contractor defense: there must be (1) a "uniquely federal interest" involved in the plaintiff's claim; and (2) a "significant conflict" between a federal

policy or interest and the operation of state law, or the application of state law must "'frustrate specific objectives' of federal legislation."[234] If both of these concerns are at play, a contractor may have an affirmative defense against state law tort claims.[235]

Although theoretically appealing, the Government contractor defense has its limits. Namely, its application largely has been limited to products liability claims and, particularly in some courts, claims involving allegedly defective military equipment.[236] Moreover, for the defense to apply, courts have required that, at the time the harm occurred, the contractor was following "reasonably precise specifications" created or approved by the Government.[237] In the area of cybersecurity, however, the Government has neither created nor approved such specifications. To the contrary, the NIST Framework, as one example, leaves contractors with considerable flexibility to apply the standards to their information systems. Even the DFARS UCTI rule requires contractors to determine whether any additional controls, beyond those enumerated in the rule, are necessary to meet the "adequate security" requirement for UCTI, without providing any guidance as to when those additional measures may be necessary.[238] For this reason, the Government contractor defense may be difficult to apply successfully in most cybersecurity litigation.

In addition to the Government contractor defense, the Supreme Court has recognized immunity for contractors engaged in public works and performing under the express authorization and direction of the United States.[239] In *Yearsley v. W.A. Ross Construction Co.*, the Supreme Court found that a contractor engaged in the construction of dikes was immune from plaintiffs' Fifth Amendment takings claims because the construction was pursuant to a valid contract with the United States.[240] Because Government officers authorized the project—and had congressional authority to do so—the contractor shared the Government's sovereign immunity against suit.[241] Although a novel argument in the cybersecurity context, it may be possible for contractors to adopt this strain of shared immunity for use in third-party suits challenging contractors' actions pursuant to Government contracts.

Finally, in certain situations, courts have extended official immunity to private actors engaged in Government functions.[242] Where contractors perform "discretionary governmental functions" pursuant to valid Government delegation, they may enjoy the absolute immunity that would otherwise apply to the governmental function had it not been delegated.[243] As in most immunity analyses, the benefits of applying the immunity must outweigh its costs.[244] Thus, this judicial extension of official immunity also may provide some protection for contractors facing cybersecurity-related litigation.

■ Public Law No. 85-804 Indemnification

As a last resort, Public Law No. 85-804[245] may, in very limited circumstances, serve as a safety net to Government contractors facing liability arising from a potential cyber attack. That statute authorizes certain federal agencies[246] to grant "extraordinary" contractual relief, including indemnification, to contractors that undertake "unusually hazardous" risks on behalf of the Government.[247] Indemnification under Public Law No. 85-804 requires a contractor to identify unusual hazards associated with the work on the Government contract for which it is performing, indicate whether it has private insurance applicable to the unusually hazardous risk, and provide details of that coverage.[248] If the indemnification request is approved, the contract is amended to include the clause at FAR 52.250-1, "Indemnification Under Public Law 85-804," which indemnifies the contractor against third-party claims, including litigation costs, to the extent the claims exceed the contractor's various insurance coverages.[249]

Indemnification under this statute is indeed "extraordinary"—it is infrequently granted.[250] Nevertheless, depending on the scope of a procurement and the potential cyber risks associated with that procurement, contractors should consider Public Law 85-804 relief as a possibility when negotiating contract terms.

Conclusion

Both the threat to information systems and the Government's approach to cybersecurity

continue to evolve, with procurements introducing new potential liabilities and complications for contractors. Government contractors must have a thorough understanding of the existing rules and regulations applicable to them and their contracts, as well as confidence that their information systems can quickly respond to and recover from a cyber attack. In the absence of a complete and consistent set of formal federal cybersecurity rules, Government contractors carry the burden of demonstrating that they have established reasonable, appropriate, and robust cybersecurity systems to protect the nation's information systems.

GUIDELINES

These *Guidelines* are intended to assist you in understanding the key legal issues and evolving compliance obligations that Government contractors face in the federal cybersecurity landscape. They are not, however, a substitute for professional representation in any specific situation.

1. *Treat cybersecurity as a matter of corporate governance and legal risk.* Cybersecurity should not be relegated to corporate IT departments. Instead, the extent of a company's cybersecurity protections and the amount of related risk it is willing to undertake are decisions that should be made by well-informed boards of directors with the advice of counsel, as they impact the entirety of an organization's health and well-being.

2. *Use the NIST Framework as a risk-assessment tool.* Though broad and open-ended, the NIST Framework represents the clearest direction the Federal Government has provided regarding adequate cybersecurity protections. Use the Framework as a baseline against which to assess an organization's current cybersecurity protections and vulnerabilities. Create current and target profiles to establish a course of action for strengthening the organization's cybersecurity systems.

3. *Understand contractual cybersecurity requirements.* While contractors should of course understand all of the terms of their contracts, they should pay particular attention to the cybersecurity requirements. Do these contract terms require the disclosure of a cybersecurity breach? Do they equitably allocate risk between the organization and the Government? Are they subject to negotiation?

4. *Know the cybersecurity requirements and risk tolerances of agency customers.* Different federal agencies have different approaches to cybersecurity, with some (e.g., the DOD) imposing significantly more stringent regulations than others. Understand each customer's cybersecurity needs and risk tolerances to ensure that the organization is in compliance with their specific requirements.

5. *Know contracting partners' cybersecurity capabilities.* The new federal cybersecurity rules impose heightened compliance and reporting requirements not only on prime contractors, but in many instances on their subcontractors as well. As a result, primes and higher tier subs should recognize that they could be held responsible for any cybersecurity issues arising from the performance of their subcontracting partners and therefore thoroughly vet their partners' and subcontractors' cybersecurity plans. Teaming and subcontracting agreements should address risks assumed by each partner such that any weak links—and data breaches resulting therefrom—are equitably allocated to the responsible party.

6. *Keep abreast of changing applicable cybersecurity requirements.* As the threats to the nation's cybersecurity continue to evolve, so too will the federal rules, regulations, and contract requirements that attempt to address them. Contractors that are aware of and in compliance with those requirements will better position themselves both for the award of future Government contracts and to respond to and mitigate any harms resulting from cyber attacks.

★ REFERENCES ★

1/ Press Release, Statement by the President on the Cybersecurity Framework (Feb. 12, 2014), http://www.whitehouse.gov/the-press-office/2014/02/12/statement-president-cybersecurity-framework.

2/ News Release, Senate Committee on Homeland Security & Governmental Affairs, Lieberman, Collins, Carper Introduce Bill To Address Serious Cyber Security Threats (Feb. 17, 2011) (remarks by Sen. Collins), http://www.hsgac.senate.gov/subcommittees/federal-financial-management/majority-media/-lieberman-collins-carper-introduce-bill-to-address-serious-cyber-security-threats.

3/ See OMB, FY 2005 Report to Congress on Implementation of the E-Government Act of 2002, at 5 (Mar. 1, 2006), available at http://georgewbush-whitehouse.archives.gov/omb/inforeg/reports/2005_e-gov_report.pdf; see also Bodenheimer & Baker, Information Security for Federal Agencies & Contractors, Briefing Papers No. 12-3, at 3 (Feb. 2012).

4/ The U.S. Government itself engages in strategic cyber attacks for national security purposes—known as "active defense" or "offensive" cyber operations—and uses private contractors in support of those projects. Such operations seek "to manipulate, disrupt, deny, degrade, or destroy information resident in computers or computer networks, or the computers and networks themselves." Gellman & Nakashima, "U.S. Spy Agencies Mounted 231 Offensive Cyber-Operations in 2011, Documents Show," Wash. Post, Aug. 30, 2013, http://www.washingtonpost.com/world/national-security/us-spy-agencies-mounted-231-offensive-cyber-operations-in-2011-documents-show/2013/08/30/d090a6ae-119e-11e3-b4cb-fd7ce041d814_story.html (quoting an unidentified presidential directive issued in October 2012). This Briefing Paper does not address those operations, which implicate a separate set of potential legal consequences for the contractors that perform or support them.

5/ Fischer, Congressional Research Service Report R42114, Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions 1 n.1 (2013).

6/ See GAO, GAO-13-187, Cybersecurity: National Strategy, Roles, and Responsibilities Need To Be Better Defined and More Effectively Implemented 4–5 & Table 1 (Feb. 14, 2013) (hereinafter "GAO Cybersecurity Report"); Securing the Modern Electric Grid From Physical and Cyber Attacks: Hearing Before the Subcomm. on Emerging Threats, Cybersec. & Sci. & Tech. of the H. Comm. on Homeland Sec., 111th Cong. 2 (2009) (Rep. Clarke, presiding); see also BAE Systems, Business and the Cyber Threat: The Rise of Digital Criminality 10 (2014), available at http://www.baesystems.com/marketoform/ Business_and_the_cyber_threat_research_NA.pdf (hereinafter "BAE Report") (listing "organized groups of fraudsters," "those involved in industrial espionage," and "hobbyist hackers" among those perceived as most likely to carry out a cyber attack).

7/ The White House has defined "critical infrastructure" as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." Exec. Order No. 13,636, § 2, 78 Fed. Reg. 11,739 (Feb. 19, 2013).

8/ See GAO Cybersecurity Report at 4-5 & Table 1.

9/ See GAO Cybersecurity Report at 4-5 & Table 1; BAE Report at 10.

10/ See Executive Office of the President, Fiscal Year 2012 Report to Congress on the Implementation of the Federal Information Security Management Act of 2002, at 30 (Mar. 2013), available at http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fy12_fisma.pdf.

11/ See GAO, GAO-12-666T, Testimony Before the Subcomm. on Oversight, Investigations, and Management, Comm. on Homeland Security, House of Representatives, Cybersecurity: Threats Impacting the Nation 8 (2012), available at http://www.gao.gov/assets/600/590367.pdf.

12/ See GAO Cybersecurity Report at 6 Table 2. A computer virus is a "computer program that can copy itself and infect a computer without the permission or knowledge of the user"; phishing is a "digital form of social engineering that uses authentic-looking, but fake, e-mails to request information from users or direct them to a fake website that requests information"; a trojan horse is a "computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms by, for example, masquerading as a useful program that a user would likely execute"; and a worm is a "self-replicating, self-propagating, self-contained program that uses network mechanisms to spread itself." GAO Cybersecurity Report at 6 Table 2.

13/ A denial of service attack allows hackers to disable a network without gaining internal access to prevent access to services on the affected network. See US-CERT, Understanding Denial-of-Service Attacks (Feb. 6, 2013), http://www.us-cert.gov/ncas/tips/ST04-015. Such attacks work by flooding access routers with fake traffic via email or transmission control protocol packets. Securosis, Defending Against Denial of Service Attacks 10 (Nov. 7, 2012), available at https://securosis.com/assets/library/reports/Securosis_Defending-Against-DoS_FINAL.pdf (hereinafter "Securosis"). Back door attacks involve unauthorized access through administrative shortcuts, configuration errors, easily deciphered passwords, and/or unsecured connections. AirMagnet, Best Practices for Rogue Detection and Annihilation 3–5 (Nov. 2004), available at http://airmagnet.flukenetworks.com/assets/whitepaper/Rogue_Detection_White_Paper.pdf (hereinafter "AirMagnet"). Hackers often find these weaknesses with the aid of computerized searchers (bots). See Securosis at 10. Rogue access points are unsecured—and, therefore, easily breached—wireless access points. See AirMagnet at 5.

14/ See Magnuson, Defense Companies Facing Array of New Cyberthreats (UPDATED), Nat'l Def. (Mar. 2014), available at http://www.nationaldefensemagazine.org/archive/2014/March/Pages/DefenseCompaniesFacingArrayofNewCyberthreats.aspx.

15/ See Executive Office of the President, Budget of the U.S. Government Fiscal Year 2014 (Apr. 10, 2013), available at http://www.gpo.gov/fdsys/pkg/BUDGET-2014-BUD/pdf/BUDGET-2014-BUD.pdf.

16/ McCarthy, Business Strategy: U.S. Federal Government IT Security Spending Forecast and Market Outlook (Dec. 2013) (summary available at http://www.idc.com/getdoc.jsp?containerId=prUS24513213).

17/ Congressional Research Service Report R42114, at 2.

18/ See 18 U.S.C.A. § 1030.

19/ See Pub. L. No. 100-235, 101 Stat. 1724 (1988). The Computer Security Act was repealed by the Federal Information Security Management Act, which is discussed in more detail below.

20/ See 44 U.S.C.A. §§ 3501–3521.

21/ See 40 U.S.C.A. § 1401 et seq.

22/ See Pub. L. No. 107-296, 116 Stat. 2135 (2002).

23/ See Pub. L. No. 107-305, 116 Stat. 2367 (2002).

24/ 44 U.S.C.A. §§ 3541–3549.

25/ 44 U.S.C.A. § 3541(1).

26/ 44 U.S.C.A. § 3541(3).

27/ 44 U.S.C. § 3543(a). The oversight authority FISMA granted to the OMB does not apply to the DOD and the Central Intelligence Agency (CIA); for those agencies, such oversight authority is assigned to the Secretary of Defense and the Director of the CIA, respectively. See 44 U.S.C.A. § 3543(c)(1). Moreover, in 2010, the OMB announced that while it would continue to maintain responsibility for FISMA's congressional reporting requirements and approval of the President's cybersecurity budget, the DHS would "exercise primary responsibility within the executive branch for the operational aspects of Federal agency cybersecurity with respect to the Federal information systems that fall within FISMA under 44 U.S.C. § 3543." Orzag & Schmidt, OMB 10-28, Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security (DHS) (July 6, 2010), available at http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-28.pdf.

28/ 44 U.S.C.A. § 3544(a)(1)(B).

29/ 44 U.S.C.A. § 3546.

30/ 44 U.S.C.A. § 3544(a). The FAR imposes additional FISMA-related mandates on agencies by requiring that procurements for IT services "comply with [FISMA's] information technology security requirements." FAR 7.103(w).

31/ 44 U.S.C.A. § 3544(b). Agencies must meet minimum security requirements by implementing appropriate security controls as described in NIST Special Publication 800-53, Rev. 4, Recommended Security Controls for Federal Information Systems (Apr. 2013, including updates as of Jan. 15, 2014), available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

32/ See 44 U.S.C.A. § 3544(b). The OMB/NIST information security standards are those "that provide minimum information security requirements as determined under section 20(b) of the National Institute of Standards and Technology Act (15 U.S.C. § 278g-3(b))," or "are otherwise necessary to improve the efficiency or operation or security of Federal information systems." 40 U.S.C.A. § 11331(b)(1)(B)(i), (ii). Those standards "shall be compulsory and binding." 40 U.S.C.A. § 11331(b)(1)(C). NIST publishes its FISMA-related policies at http://csrc.nist.gov/groups/SMA/fisma/.

33/ 44 U.S.C.A. § 3544(a)(1)(A)(ii).

34/ See GAO, GAO-13-776, Federal Information Security: Mixed Progress in Implementing Program Components; Improved Metrics Needed to Measure Effectiveness (Sept. 26, 2013) (hereinafter "GAO FISMA Implementation Report")

35/ GAO FISMA Implementation Report at 45.

36/ GAO FISMA Implementation Report at 45. The GAO's report also noted that the OMB and the DHS, the two agencies charged with oversight of agency FISMA implementation efforts, had failed to establish performance metrics to track those efforts, "making it more difficult to accurately assess the extent to which agencies are effectively securing their systems," and resulting in a lack of "visibility into the federal government's information security posture." GAO FISMA Implementation Report at 45.

37/ See 76 Fed. Reg. 38,089 (June 29, 2011).

38/ DOD, Safeguarding Unclassified Controlled Technical Information (Oct. 10, 2013), available at http://www.defense.gov/documents/Signed_DVTT_Memo_101013.pdf.

39/ 78 Fed. Reg. 69,273 (Nov. 18, 2013) (adding DFARS subpt. 204.73 and the clause at DFARS 252.204-7012). The scope of the proposed DFARS rule encompassed all unclassified DOD information; however, the final UCTI rule was narrowed to cover only DOD UCTI. See 78 Fed. Reg. 69,273.

40/ DFARS 252.204-7012(a). The UCTI rule explains that it does not apply to "information that is lawfully publicly available without restrictions" and directs that controlled technical information shall be "marked with one of the distribution statements B-through-F, in accordance with DOD Instruction 5230.24, Distribution Statements on Technical Documents." DFARS 252.204-7012(a).

41/ See DFARS 252.204-7012(b), (d).

42/ DFARS 204.7303.

43/ 78 Fed. Reg. at 69,274-75.

44/ DFARS 252.204-7012(a).

45/ DFARS 252.204-7012(b)(1)(i). Those 14 areas are access control; audit and accountability; awareness and training; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; program management; risk assessment; system and communications protections; and system and information integrity. See DFARS 252.204-7012(b)(1)(i) (Table 1).

46/ DFARS 252.204-7012(b)(1)(ii).

47/ See DFARS 252.204-7012(b)(2); see also 78 Fed. Reg. at 69,276 (noting that the rule does not require contractors to conduct a specific analysis to determine if additional controls are reasonably necessary, but requires contractors that are aware of a risk or vulnerability to address that shortcoming).

48/ DFARS 252.204-7012(d). "Cyber incident" is defined as "actions taken through the use of computer networks that result in an actual or potentially adverse effect on information systems and/or the information residing therein." DFARS 252.204-7012(a).

49/ DFARS 252.204-7012(d)(4)(iii).

50/ DFARS 252.204-7012(d)(5). The rule suggests that even a mere "inadvertent release" of data could trigger its reporting requirements. See DFARS 252.204-7012(d)(1)(xi).

51/ DFARS 252.204-7012(d)(1). Contractors must report "as much of the following information as can be obtained": "(i) Data Universal Numbering System; (ii) Contract numbers affected unless all contracts by the company are affected; (iii) Facility CAGE code if the location of the event is different than the prime Contractor location; (iv) Point of contact if different than the POC recorded in the System for Award Management (address, position, telephone, email); (v) Contracting Officer point of contact (address, position, telephone, email); (vi) Contract clearance level; (vii) Name of subcontractor and CAGE code if this was an incident on a Sub-contractor network; (viii) DOD programs, platforms or systems involved; (ix) Location(s) of compromise; (x) Date incident discovered; (xi) Type of compromise (e.g., unauthorized access, inadvertent release, other); (xii) Description of technical information compromised; and (xiii) Any additional information relevant to the information compromise." DFARS 252.204-7012(d)(1).

52/ DFARS 252.204-7012(d)(5). The scope of the disclosure exception is unclear, and as a result, contractors may face difficult questions regarding whether to disclose privileged or third-party proprietary information. Prudent contractors should consider revising their contractual agreements with business partners to address these disclosure requirements and institute a system for reviewing compromised files in short order to determine any existing disclosure limitations.

53/ DFARS 252.204-7012(d)(4)(i)–(ii).

54/ DFARS 252.204-7012(d)(4)(iii).

55/ DFARS 252.204-7012(g).

56/ See 77 Fed. Reg. 51,496, 51,497 (Aug. 24, 2012).

57/ See 77 Fed. Reg. 51,496, 51,498. The scope of the proposed FAR rule includes solicitations and contracts for commercial items and commercially available off-the-shelf items. See 77 Fed. Reg. 51,496, 51,498.

58/ 77 Fed. Reg. at 51,499.

59/ 77 Fed. Reg. at 51,499.

60/ 77 Fed. Reg. at 51,499.

61/ The offices and agencies that comprise the IC are identified at 50 U.S.C.A. § 3003(4).

62/ See 50 U.S.C.A. § 3329 note (IC); National Defense Authorization Act for Fiscal Year 2014, Pub. L. No. 113-66, § 3113, 127 Stat. 672, 1053 (2013) (adding 50 U.S.C.A. § 2786) (DOE); National Defense Authorization Act for Fiscal Year 2011, Pub. L. No. 111–383, § 806, 124 Stat. 4137, 4260 (2011), as amended by National Defense Authorization Act for Fiscal Year 2013, Pub. L. No. 112–239, § 806, 126 Stat. 1632, 1827 (2013) (DOD); see also 78 Fed. Reg. 69,268, 69,273 (Nov. 18, 2013) (DFARS implementation of the DOD authority).

63/ See 50 U.S.C.A. § 3329 note; 50 U.S.C.A. § 2786(f)(6); DFARS 252.239-7018(a).

64/ See 50 U.S.C.A. § 3329 note; 50 U.S.C.A. § 2786(f)(4); DFARS 239.7305.

65/ See 50 U.S.C.A. § 2786(f)(4).

66/ See 50 U.S.C.A. § 3329 note; 50 U.S.C.A. § 2786(b); DFARS 239.7303(a), 239.7304(c).

67/ See 50 U.S.C.A. § 3329 note; 50 U.S.C.A. § 2786(c); DFARS 239.7305(d).

68/ The grant to the DOD of enhanced authority explicitly so states. See DFARS 252.239-7018(d). Given the similarity of the grants of enhanced authority to the three Executive Branch components, the DOE's and the IC's exercise of enhanced authority also would likely be unreviewable in a bid protest because those entities may rely on national security concerns as a basis for limiting disclosure.

69/ The DFARS UCTI rule permits the Government to provide information about cybersecurity incidents to authorized persons "for purposes and activities consistent with this clause." DFARS 252.204-7012(e). That broad language would not necessarily prevent an agency from considering cybersecurity breaches when determining whether a contractor poses a supply chain risk.

70/ A "high-impact" information system is one in which "the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals." High-impact information systems typically hold the Government's classified information. See NIST, FIPS Pub 199, Standards for Security Categorization of Federal Information and Information Systems 3 (2004), available at http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf (hereinafter "NIST Publication 199").

71/ A "moderate-impact" information system is one in which the "loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals." See NIST Publication 199, at 2. Moderate-impact information systems typically hold much of the Government's unclassified information.

72/ Pub. L. No. 113-76, § 515(a), 128 Stat. 5, 80 (2014).

73/ Pub. L. No. 113-76, § 515(b).

74/ See Pub. L. No. 112-81, § 818(a)–(c), 125 Stat. 1298, 1493 (2011).

75/ See Pub. L. No. 112-239, § 833, 126 Stat. 1632, 1844 (2013).

76/ See DOD Instruction No. 4140.67, DOD Counterfeit Prevention Policy (Apr. 26, 2013), available at http://www.dtic.mil/whs/directives/corres/pdf/414067p.pdf (hereinafter "Counterfeit Prevention Policy").

77/ 78 Fed. Reg. 28,780 (May 1, 2013).

78/ 79 Fed. Reg. 26,092 (May 6, 2014).

79/ The Counterfeit Prevention Policy defines "counterfeit materiel" as an "item that is an unauthorized copy or substitute that has been identified, marked, or altered by a source other than the item's legally authorized source and has been misrepresented to be an authorized item of the legally authorized source." Counterfeit Prevention Policy at 12 (Glossary).

80/ "Supply chain" is defined as "[t]he linked activities associated with providing materiel from a raw material stage to an end user as a finished product or system, including design, manufacturing, production, packaging, handling, storage, transport, mission operation, maintenance, and disposal." Counterfeit Prevention Policy at 13 (Glossary).

81/ Counterfeit Prevention Policy at 1.

82/ Counterfeit Prevention Policy at 12 (Glossary).

83/ See Counterfeit Prevention Policy at 2. This same "risk based" approach is reflected in the final DFARS rule.

84/ 79 Fed. Reg. 26,092.

85/ See National Defense Authorization Act for Fiscal Year 2013, Pub. L. No. 112-239, § 833, 126 Stat. 1632, 1844 (2013) (amending Pub. L. No. 112-81, § 818).

86/ 79 Fed. Reg. at 26,093–96, 26,106, 26,108; DFARS 252.246-7007(a).

87/ 79 Fed. Reg. at 26,106; see DFARS 252.246-7007.

88/ 79 Fed. Reg. at 26,106; DFARS 231.205-71(b). FY 2013 NDAA § 833 statutorily imposes the exceptions to cost unallowability. See Pub. L. No. 112-239, § 833.

89/ 79 Fed. Reg. at 26,093; DFARS 246.870-3(a)

90/ 79 Fed. Reg. at 26,106, 26,108; DFARS 246.870-2(a), 252.246-7007(b).

91/ 79 Fed. Reg. at 26,106-08; DFARS 246.870-2(b), 252.246-7007(c).

92/ 79 Fed. Reg. at 26,106, 26,108; DFARS 246.870-2(a), 252.246-7007(b).

93/ 79 Fed. Reg. at 26,106, 26,108; DFARS 246.870-2(a), 252.246-7007.

94/ See 79 Fed. Reg. at 26,099, 26,106, 26,108; DFARS 246.870-2(a), 252.246-7007(c)(9), (e).

95/ 79 Fed. Reg. at 26,099.

96/ See 79 Fed. Reg. at 26,099, 26.106, 26,108; DFARS 246.870-2(a), 252.246-7007(c)(9), (e).

97/ Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 19, 2013).

98/ Presidential Policy Directive 21, Critical Infrastructure Security and Resilience (Feb. 12, 2013), http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (hereinafter "PPD 21").

99/ E.O. 13636 § 7.

100/ E.O. 13636 § 8(d).

101/ E.O. 13636 § 4.

102/ E.O. 13636 § 8(e).

103/ PPD 21.

104/ PPD 21.

105/ PPD 21.

106/ See E.O. 13636 § 8(e).

107/ E.O. 13636 § 8(e).

108/ GSA & DOD, Improving Cybersecurity and Resilience Through Acquisition (Nov. 2013) (released publicly on Jan. 23, 2014), available at http://www.defense.gov/news/Improving-Cybersecurity-and-Resilience-Through-Acquisition.pdf (hereinafter "Joint Report").

109/ Joint Report at 3.

110/ Joint Report at 13–14.

111/ Joint Report at 14–15.

112/ Joint Report at 15.

113/ Joint Report at 15–17.

114/ Joint Report at 17–18. Criteria for determining whether a supplier is "trusted" include: long-term business viability, quality control systems, order placement and fulfillment processes, customer support, customer return policies, and past record, such as by a search in the Government-Industry Data Exchange Program. See Joint Report at 18. This recommendation recognizes that its implementation could limit competition and, as a result, suggests limiting the requirements to high-risk acquisitions. See Joint Report at 18.

115/ Joint Report at 19–20.

116/ See Joint Report at 7.

117/ See 79 Fed. Reg. 14,042 (Mar. 12, 2014).

118/ See Joint Working Group on Improving Cybersecurity and Resilience Through Acquisition, Draft Implementation Plan (Feb. 2014), available at http://www.gsa.gov/portal/content/176547 (hereinafter "Draft Implementation Plan").

119/ Draft Implementation Plan at 4.

120/ See Draft Implementation Plan.

121/ See 79 Fed. Reg. 14,042.

122/ See 32 C.F.R. pt. 236. The DOD issued a final rule establishing the current version of the DIB CS/IA program in October 2013. See 78 Fed. Reg. 62,430 (Oct. 22, 2013).

123/ See 78 Fed. Reg. 62,430.

124/ See DOD, Fact Sheet: Defense Industrial Base Cybersecurity Activities May 11, 2012, available at http://www.defense.gov/news/d20120512dib.pdf (hereinafter "DOD Fact Sheet").

125/ See DOD Fact Sheet.

126/ See 32 C.F.R. § 236.4(a).

127/ See Perera, DoD Finalizes Cybersecurity Two-Way Threat Sharing Program Regulations, FierceGovernmentIT (Oct. 23, 2013), http://www.fiercegovernmentit.com/story/dod-finalizes-cybersecurity-two-way-threat-sharing-program-regulations/2013-10-23.

128/ E.O. 13636 § 4(a), (c).

129/ DHS, Enhanced Cybersecurity Services, http://www.dhs.gov/enhanced-cybersecurity-services (hereinafter "Enhanced Cybersecurity Services").

130/ Enhanced Cybersecurity Services.

131/ Enhanced Cybersecurity Services.

132/ NIST, Framework for Improving Critical Infrastructure Cybersecurity (Feb. 12, 2014), available at http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf (hereinafter "Framework Version 1.0"). This finalized version of the Framework follows a preliminary version of the Framework issued in October 2013. See NIST, Improving Critical Infrastructure Cybersecurity, Executive Order 13636: Preliminary Cybersecurity Framework (Oct. 22, 2013), available at http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf (hereinafter "Preliminary Framework").

133/ Those identified sectors are Chemical, Commercial Facilities, Communications, Critical Manufacturing, Dams, Defense Industrial Base, Emergency Services, Energy, Financial Services, Food and Agriculture, Government Facilities, Healthcare and Public Health, Information Technology, Nuclear Reactors, Materials and Waste, Transportation Systems, and Water and Wastewater. See PPD 21.

134/ Framework Version 1.0, at 3.

135/ Framework Version 1.0, at 1.

136/ Framework Version 1.0, at 5.

137/ Framework Version 1.0, at 8–9.

138/ Framework Version 1.0, at 8.

139/ See Framework Version 1.0, at 19–36.

140/ See Framework Version 1.0, at 9.

141/ Framework Version 1.0, at 10.

142/ Framework Version 1.0, at 10.

143/ Framework Version 1.0, at 10.

144/ Framework Version 1.0, at 10.

145/ Framework Version 1.0, at 10.

146/ Framework Version 1.0, at 11.

147/ Framework Version 1.0, at 11.

148/ Framework Version 1.0, at 9.

149/ Framework Version 1.0, at 9.

150/ Framework Version 1.0, at 11.

151/ Framework Version 1.0, at 11.

152/ Framework Version 1.0, at 11.

153/ Framework Version 1.0, at 11.

154/ Framework Version 1.0, at 11.

155/ Framework Version 1.0, at 11.

156/ Framework Version 1.0, at 1, 13.

157/ Framework Version 1.0, at 2.

158/ Framework Version 1.0, at 13 ("Utilizing the Framework as a cybersecurity risk management tool, an organization can determine activities that are most important to critical service delivery and prioritize expenditures to maximize the impact of the investment.").

159/ Framework Version 1.0, at 15–17. E.O. 13636 directed NIST to address privacy and civil liberty concerns as part of any proposed cybersecurity initiative. See E.O. 13636 § 5. To address such concerns, the Framework directs that organizations consider how their cybersecurity programs can incorporate privacy principles, explaining that "privacy and civil liberties implications may differ by sector or over time and organizations may address these considerations and processes with a range of technical implementations." Framework Version 1.0, at 15.

160/ Framework Version 1.0, at 2.

161/ NIST, Roadmap for Improving Critical Infrastructure Cybersecurity (Feb. 12, 2014), available at http://www.nist.gov/cyberframework/upload/roadmap-021214.pdf (hereinafter "NIST Roadmap").

162/ NIST Roadmap at 1.

163/ NIST Roadmap at 2.

164/ NIST Roadmap at 3–9.

165/ NIST Roadmap at 2.

166/ Joint Report at 13.

167/ Framework Version 1.0, at 15.

168/ Framework Version 1.0, at 15.

169/ See Framework Version 1.0, at 13; DHS, C^3 Voluntary Program: Cyber Risk Management Primer for CEOs, available at http://www.us-cert.gov/sites/default/files/c3vp/ccubedvp-outreach-and-messaging-kit.pdf (listing, among other things, "5 Questions CEOs Should Ask About Cyber Risks").

170/ 65 C.J.S. Negligence § 115.

171/ See 65 C.J.S. Negligence § 115.

172/ Indeed, the Framework holds itself out as a compilation of already existing norms. See, e.g., Framework Version 1.0, at 1 ("The Framework provides organization and structure to today's multiple approaches to cybersecurity by assembling standards, guidelines, and practices that are working effectively in industry today.").

173/ E.O. 13636 anticipates that agencies may promulgate new enforcement mechanisms based on the Framework. See E.O. 13636 § 10.

174/ See 65 C.J.S. Negligence §§ 111, 136.

175/ See 65 C.J.S. Negligence §§ 111, 133–134.

176/ Boyd v. Moore, 919 N.E.2d 283, 287 (Ohio Ct. App. 2009) (internal quotation marks and alteration omitted); see also 65 C.J.S. Negligence § 111.

177/ See, e.g., Framework Version 1.0, at 4 ("The Framework complements, and does not replace, an organization's risk management process and cybersecurity program. The organization can use its current processes and leverage the Framework to identify opportunities to strengthen and communicate its management of cybersecurity risk while aligning with industry practices. Alternatively, an organization without an existing cybersecurity program can use the Framework as a reference to establish one.").

178/ Framework Version 1.0, at 7.

179/ DHS, C^3 Voluntary Program: Frequently Asked Questions, available at http://www.us-cert.gov/sites/default/files/c3vp/ccubedvp-outreach-and-messaging-kit.pdf.

180/ See, e.g., Framework Version 1.0, at 2 ("This Framework is not a one-size-fits-all approach to managing cybersecurity risk for critical infrastructure."), 6 ("The Framework is adaptive to provide a flexible and risk-based implementation….").

181/ Framework Version 1.0, at 1.

182/ See, e.g., Framework Version 1.0, at 12 (contemplating communication of "mission priorities, available resources, and overall risk tolerance" from the executive level to the business/process level), 24 ("Senior executives understand roles & responsibilities.").

183/ Framework Version 1.0, at 13.

184/ See BAE Report at 5, 14.

185/ See BAE Report at 17.

186/ See generally World Economic Forum, Risk and Responsibility in a Hyperconnected World (Jan. 2014), available at http://www.mckinsey.com/insights/business_technology/~/media/mckinsey/dotcom/insights/business%20technology/risk%20and%20responsibility%20in%20a%20hyperconnected%20world%20implications%20for%20enterprises/risk%20and%20responsibility%20in%20a%20hyperconnected%20world.ashx.

187/ See generally FAR subpt. 49.4.

188/ See FAR 9.104-1.

189/ See FAR 15.305.

190/ See 50 U.S.C.A. § 3329 note (IC); Pub. L. No. 113-66, § 3113 (DOE); DFARS subpt. 239.73 (DOD).

191/ See generally American Bar Association Committee on Debarment and Suspension, Practitioner's Guide to Suspension and Debarment (3d ed. 2002); Shaw, Wagner & Nichols, "Contractor Responsibility: Toward an Integrated Approach to Legal Risk Management," Briefing Papers No. 13-4 (Mar. 2013); West, Hatch, Brennan & VanDyke, "Suspension & Debarment," Briefing Papers No. 06-9 (Aug. 2006).

192/ See FAR 9.406-2(b) (debarment); FAR 9.407-2(a) (suspension).

193/ FAR 9.406-2(c); accord FAR 9.407-2(c).

194/ See FAR 9.406-1(b)–(c); FAR 9.407-1(c)–(d). In the event of debarment, a contractor may continue to perform under an existing contract, but an agency may not extend or renew the contract, nor issue task orders against the contract, unless the agency's head "states in writing the compelling reasons justifying continued business dealings between that agency and the contractor." FAR 9.406-1(c).

195/ Several states provide for reciprocal suspension or debarment based on suspension or debarment by the Federal Government or another state. See Mass. Gen. Laws Ann. ch. 29, § 29F(c)(2) (federal); Md. Code Ann. State Fin. & Proc. § 16-203(c) (federal); N.J. Admin. Code § 17:19-4.1(a)(13) ("any other agency of government"); Ohio Rev. Code Ann. § 153.02(A)(9) (federal or other state); 62 Pa. Cons. Stat. Ann. § 531(b)(9) (federal or other state); Va. Dep't of Transp., Debarment and/or Suspension Policy 3 (as amended Aug. 2, 1995), available at http://www.vamegaprojects.com/tasks/sites/default/assets/File/pdf/Exhibit_D_debarment_procedures.pdf (federal or other state).

196/ 31 U.S.C.A. §§ 3729–3733.

197/ 31 U.S.C.A. § 3729(a)(1)(A)–(B).

198/ See, e.g., United States v. Mass. Hous. Fin. Agency, 530 F.3d 980, 983 (D.C. Cir. 2008) (internal quotation marks omitted); United States v. Krizek, 111 F.3d 934, 941–42 (D.C. Cir. 1997).

199/ Ebeid v. Lungwitz, 616 F.3d 993, 996–98 (9th Cir. 2010) (internal quotation marks omitted). See generally Shaw, Wagner & Nichols, "Contractor Responsibility: Toward an Integrated Approach to Legal Risk Management," Briefing Papers No. 13-4 (Mar. 2013); Mitchell, Abbott & Orozco, "Implied Certification Liability Under the False Claims Act," Briefing Papers No. 11-4 (Mar. 2011).

200/ Moreover, to the extent that such mistaken belief in its ability to comply with cybersecurity requirements is conveyed to the Government and serves as the basis for the Government's decision to award a contract, it could also give rise to an FCA violation under the less common but still utilized theory of "fraud-in-the-inducement." See, e.g., Harrison v. Westinghouse Savannah River Co., 176 F.3d 776, 787–88 (4th Cir. 1999), 41 GC ¶ 317.

201/ As an example, US Investigations Services LLC, "the company that vetted Edward Snowden," is facing allegations of violating the FCA, as well as a possible suspension from Government contracting, over its alleged failure to perform adequate personnel investigations. See Salant & Miller, "Snowden Vetter Risks U.S. Contract Ban," Bloomberg (Feb. 11, 2014 2:51 PM ET), http://www.bloomberg.com/news/2014-02-11/snowden-vetter-risks-u-s-contract-ban.html.

202/ DFARS 252.204-7012(g).

203/ DFARS 252.204-7012(d), (g). See 78 Fed. Reg. 69,273, 69,278 (Nov. 18, 2013).

204/ U.S. Department of Interior, Solicitation No. D12PS00316, § H.12 (June 18, 2012) available at https://www.fbo.gov/index?s=opportunity&mode=form&id=a6c194b6f4b550970d03c699a8f02304&tab=core&tabmode=list&=.

205/ See Pub. L. No. 112-239, § 941, 126 Stat. 1632, 1889 (2013) (modifying the DOD DIB CS/IA program to mandate the reporting of cyber intrusion incidents by cleared defense contractors).

206/ See, e.g., Sources Sought Notice for U.S. Department of Veterans Affairs Technology Acquisition Center Solicitation No. VA118-11-RI-0377, Addendum B, § B6, available at https://www.fbo.gov/index?s=opportunity&mode=form&id=0eeea93d6347204f98159e7e1254d233&tab=core&_cview=1 (requiring "security incident" reporting).

207/ See National Conference of State Legislators, State Security Breach Notification Laws, http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (last updated Apr. 11, 2014).

208/ See SEC Division of Corporation Finance, CF Disclosure Guidance: Topic No. 2 Cybersecurity (Oct. 13, 2011), http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm (hereinafter "CF Disclosure Guidance—Cybersecurity").

209/ See CF Disclosure Guidance—Cybersecurity.

210/ 48 C.F.R. § 552.239-71(k).

211/ See, e.g., U.S. Office of Personnel Management, Solicitation No. OPM13-13-Q-0001 (May 17, 2013), available at https://www.fbo.gov/index?s=opportunity&mode=form&id=a909de73d18bf02aa99a214c49b8c01f&tab=core&_cview=0.

212/ See Office of Inspector General, DHS, Evaluation of DHS' Information Security Program for Fiscal Year 2013, OIG-14-09, App. M (Nov. 2013), available at http://www.oig.dhs.gov/assets/Mgmt/2014/OIG_14-09_Nov13.pdf.

213/ 78 Fed. Reg. 69,273, 69,274 (Nov. 18, 2013).

214/ See Pub. L. No. 112-239, § 941(c)(2)(A), 126 Stat. 1632, 1889 (2013).

215/ See DCAA, About DCAA, http://www.dcaa.mil/about_dcaa.html.

216/ DCAA Contract Audit Manual ¶ 5-102(b) (July 30, 2013), available at http://www.dcaa.mil/cam/Chapter_05_-_Audit_of_Accounting_and_Management_Systems.pdf (internal quotation marks omitted).

217/ SEC National Exam Program, Office of Compliance Inspections and Examinations, Examination Priorities for 2013, at 3 (Feb. 21, 2013), available at http://www.sec.gov/about/offices/ocie/national-examination-program-priorities-2013.pdf; see also SEC National Exam Program, Office of Compliance Inspections and Examinations, Examination Priorities for 2014, at 2 (Jan. 9, 2014), available at http://www.sec.gov/about/offices/ocie/national-examination-program-priorities-2014.pdf ("The [SEC] will continue to examine governance and supervision of information technology systems,... information security, and preparedness to respond to sudden malfunctions and system outages.").

218/ See FAR pt. 31.

219/ CF Disclosure Guidance—Cybersecurity.

220/ See CF Disclosure Guidance—Cybersecurity.

221/ See 78 Fed. Reg. 69,273, 69,274 (Nov. 18, 2013).

222/ FAR 31.201-3(a) provides that "[a] cost is reasonable if, in its nature and amount, it does not exceed that which would be incurred by a prudent person in the conduct of competitive business."

223/ See Willhite, More CFOs Weigh Cyber-Risk Insurance, Wall St. J. (Aug. 13, 2013).

224/ See, e.g., Retail Ventures, Inc. v. Nat'l Union Fire Ins. Co. of Pittsburgh, 691 F.3d 821 (6th Cir. 2012).

225/ Pub. L. No. 107-296, 116 Stat. 2135 (2002).

226/ Pub. L. No. 107-296, §§ 861–865 (codified at 6 U.S.C.A. §§ 441–444).

227/ See 71 Fed. Reg. 33,147 (June 8, 2006).

228/ See DHS, SAFETY Act Approved Technologies, https://www.safetyact.gov/jsp/award/samsApprovedAwards.do?action=SearchApprovedAwardsPublic.

229/ 6 U.S.C.A. § 444(2).

230/ See H.R. 3696 § 202, 113th Cong. (2013).

231/ H.R. 3696 § 202(a)(4).

232/ Boyle v. United Techs. Corp., 487 U.S. 500, 507 (1988).

233/ Boyle, 487 U.S. 500.

234/ Boyle, 487 U.S. at 504–07.

235/ Boyle, 487 U.S. at 507–08.

236/ See, e.g., Boyle, 487 U.S. at 512; In re Haw. Fed. Asbestos Cases, 960 F.2d 806, 810–12 (9th Cir. 1992); 72A C.J.S. Products Liability § 82 (updated Mar. 2014). But see Carley v. Wheeled Coach, 991 F.2d 1117, 1119–25 (3d Cir. 1993) (finding defense available against claim by emergency medical technical injured in ambulance accident); Russek v. Unisys Corp., 921 F. Supp. 1277, 1286–87 (D.N.J. 1996) (finding defense available against claims by postal workers alleging injuries caused by letter-sorting machines); Wisner v. Unisys Corp., 917 F. Supp. 1501, 1509–10 (D. Kan. 1996) (same); Johnson v. Grumman Corp., 806 F. Supp. 212, 215–17 (W.D. Wis. 1992) (finding defense available against claim by individual injured while working on a postal truck).

237/ Boyle, 487 U.S. at 512.

238/ See DFARS 252.204-7012(b)(2).

239/ See Yearsley v. W.A. Ross Constr. Co., 309 U.S. 18, 20–21 (1940).

240/ See Yearsley, 309 U.S. at 19–21.

241/ See Yearsley, 309 U.S. at 20–21; see also Ackerson v. Bean Dredging LLC, 589 F.3d 196, 204–07 (5th Cir. 2009) (applying Yearsley immunity to a suit against contractors engaged in dredging activities following Hurricane Katrina).

242/ See Mangold v. Analytic Servs., Inc., 77 F.3d 1442, 1447–50 (4th Cir. 1996); see also Westfall v. Erwin, 484 U.S. 292, 295–98 & n.3 (1988), superseded by statute, 28 U.S.C.A. § 2679(d); Pani v. Empire Blue Cross Blue Shield, 152 F.3d 67, 72 (2d Cir. 1998) (explaining that "the Westfall test remains the framework for determining when nongovernmental persons or entities are entitled to [official] immunity").

243/ Mangold, 77 F.3d at 1447–49 (extending official immunity to a contractor "insofar as necessary to shield statements and information, whether truthful or not, given by a government contractor and its employees in response to queries by government investigators engaged in an official investigation"); see also Murray v. Northrop Grumman Info. Tech., Inc., 444 F.3d 169, 174–76 (2d Cir. 2006) (extending official immunity to a "contractor, hired to perform a quintessential governmental function," and which, "in the course of its official duties convey[ed] information with possible national security implications to the agency charged with its oversight").

244/ See Westfall, 484 U.S. at 295–96, 299; Mangold, 77 F.3d at 1446–47.

245/ Pub. L. No. 85-804, 72 Stat. 972 (1958) (codified at 50 U.S.C.A. § 1431 et seq.); see FAR subpt. 50.1. See generally Mullen, "Extraordinary Contractual Relief Under Public Law 85-804," Briefing Papers No. 02-13 (Dec. 2002).

246/ The agencies authorized to consider 85-804 relief are identified at FAR 50.101-1(b).

247/ See Exec. Order No. 10789, 23 Fed. Reg. 8897, § 1A(a) (1958); FAR 52.250-1.

248/ See FAR 50.104-3.

249/ FAR 52.250-1.

250/ See Dover & McGovern, Risk Mitigation Approaches for Government Contractors, Briefing Papers No. 07-5, at 2 (Apr. 2007).