BRIEFING PAPERS® SECOND SERIES

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

Cybersecurity & Critical Infrastructure

*By Melinda R. Biancuzzo**

Nation-states are increasingly using cyber as an offensive tool to collect business information that will enhance their competitive standing and military and diplomatic information to gain an advantage in negotiations or strategic decisions.[1] Targets range from government institutions, to industrial facilities, and to private businesses. Nation-state hacking techniques run the gamut, from sophisticated malware tools to simpler, off-the-shelf tools. In many attacks, however, the common element is the exploitation of human individuals within an organization. This is often referred to as an "insider threat," which is broadly defined to include both intentional actions (e.g., Edward Snowden) and unintentional actions, such as improper or accidental disposal of physical records (e.g., failing to shred a document with your network login information and password), falling victim to a phishing email attack, or losing your laptop or other data storage device. As insiders tend to be the path of least resistance for cyber attacks, government contractors are in the cross-hairs regardless of whether they are operating the government's information technology (IT) networks or simply have access to sensitive information. Those operating in one or more of the nation's "critical infrastructure" face an even greater risk. This BRIEFING PAPER explores critical infrastructure cybersecurity specific to the U.S. Defense Industrial Base (DIB).

Defining Critical Infrastructure

The Critical Infrastructures Protection Act of 2001 defines "critical infrastructure" to mean "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."[2] Officially, there are 16 "sectors" that the U.S. Government deems "critical infrastructure":

- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing

*Melinda R. Biancuzzo is an associate in Gibson Dunn's Washington, D.C. office with a practice co-specialized in both Government Contracts and Cybersecurity and Data Privacy.

IN THIS ISSUE:

- 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
- Water and Wastewater Systems[3]

A 2015 report from the University of Cambridge Centre for Risk Studies and the Lloyd's of London insurance market estimated the impact if hackers were to shut down the power grid in 15 U.S. states and Washington, D.C. and leaving 93 million people without power:

> Experts predict [a shutdown by hackers] would result in a rise in mortality rates as health and safety systems fail; a decline in trade as ports shut down; disruption to water supplies as electric pumps fail and chaos to transport networks as infrastructure collapses.
>
> The total impact to the US economy is estimated at $243 billion, rising to more than $1 trillion in the most extreme version of the scenario. The cyber attack scenario shows the broad range of claims that could be triggered by disruption to the US power grid, with total amount of claims paid by the insurance industry estimated at $21.4 billion, rising to $71.1 billion in the most extreme version of the scenario.[4]

With the increasing prevalence of hostile nation-states and advanced persistent threats targeting U.S. interests, critical infrastructure sectors are targeted more frequently than ever before. While critical infrastructure has been a cyber priority for the Executive Branch and Congress, the overarching policies for critical infrastructure are voluntary and cybersecurity of critical infrastructure systems and assets is not uniformly protected or regulated across all 16 sectors.

In fact, the most heavily regulated sectors in terms of cybersecurity are privacy-focused rather than security-focused. Compare, for example, contractors operating in the healthcare sector with the transportation sector. Healthcare sector contractors—*e.g.*, Department of Veterans Affairs contracts with medical professionals, medical device manufacturers, or insurance companies—are heavily regulated by both the Department of Health and Human Services as well as the Federal Trade Commission by virtue of their access to personal health information (PHI), in addition to any agency-specific requirements imposed by the contract. In contrast, regulators appear to have taken a "come what may" approach to cybersecurity in the transportation sector. While cyber initiatives are in progress for the automotive industry,[5] the focus to date has been limited to the automotive manufacturer, completely disregarding other vulnerabilities in the supply chain, such as the dealership that maintains the electronic data, the vendors that might have access to the dealership management system, and so on. Beyond that, the security model for other forms of transportation like airplanes—even post-9/11—remains focused on the physical threat rather than the cyber threat. The disparity here especially is alarming if you consider that most modern transportation operates with the support of connected computer systems. Much of this can be explained by the pendulum swing post-Snowden away from national surveillance and towards individual privacy. But, beginning in 2015, that pendulum began swinging back towards national security concerns, especially in the cybersecurity sphere following

Editor: Valerie L. Gross

Briefing Papers® (ISSN 0007-0025) is published monthly, except January (two issues) and copyrighted by Thomson Reuters, 610 Opperman Drive, P.O. Box 64526, St. Paul, MN 55164-0526. Customer Service: (800) 328-4880. Periodical Postage paid at St. Paul, MN. POSTMASTER: Send address changes to Briefing Papers, 610 Opperman Drive, P.O. Box 64526, St. Paul, MN 55164-0526.

the San Bernardino and Paris shootings. Indeed, a Pew Research Center survey in December 2016 found that 56% of Americans were more concerned that the government's anti-terror policies did not go far enough to protect the country, compared with 28% who expressed concern that the policies went too far in restricting the average person's civil liberties.[6]

The purpose of this BRIEFING PAPER is not to belabor the varying degrees of incongruities or the nuances between each sector, but to provide a roadmap for navigating the complex sector-specific requirements and provide best practices for mitigating the cybersecurity risks contractors operating within the critical infrastructure will face. This PAPER specifically focuses on those issues for the Defense Industrial Base.

The Risks

According to a recent report, the top three causes of cyber incidents in the public sector during 2016 were cyber-espionage, misuse of privileges (primarily by insiders), and unintentional errors that directly compromised security.[7] Of the public sector attacks resulting in confirmed data disclosure, almost one half were reportedly state-affiliated attacks.[8] One technique often used by foreign states is referred to as an advanced persistent threat (APT), which uses multiple phases to get into a network, avoid detection, and continue to collect valuable information over the long term.[9]

There are several motives for foreign state cyber attacks. Foreign states use cyber tools as part of their information gathering and espionage activities, including economic espionage directed against U.S. businesses. In addition, several nations, including Russia, China, and North Korea, are aggressively working to incorporate cyber expertise as part of their "information warfare" programs and capabilities.[10] Information warfare is a concept that uses computer network operations, electronic warfare, psychological operations, and information operations to control the information landscape in order to achieve political objectives both at home and abroad.[11] For example, hostile nations engage in industrial control system attacks that are intended to disrupt or destroy activities of large-scale companies, utilities, and organizations. Russia reportedly has been successful in launching numerous attacks against its enemies' critical infrastructure sectors, including taking down Ukraine's power grid and shutting down 12 news stations in France.[12]

The common vector for many attacks is the exploitation of the human element (i.e., the "weakest link") within an organization.[13] Thus, by virtue of contractors' access to federal systems and information—from military systems to trade secrets to personally identifiable information—government contractors are an appealing threat vector for a foreign state to exploit. And contractors operating in or with access to a critical infrastructure sector are particularly at risk because the potential damage from a cyber attack on critical infrastructure is so high.

Policy Framework

U.S. Agency Oversight & Responsibilities

The Department of Homeland Security (DHS) leads the Federal Government's efforts to secure U.S. critical infrastructure and works with owners and operators to prepare for, prevent, mitigate, and respond to threats. In addition, at least one federal agency is assigned to oversee each critical infrastructure sector. These agencies are known as "Sector-Specific Agencies." The U.S. Department of Defense (DOD) is the Sector-Specific Agency for the Defense Industrial Base sector.[14] Each Sector-Specific Agency is responsible for developing, in coordination with its public and private sector partners, a Sector-Specific Plan that details how the National Infrastructure Protection Plan risk management framework is implemented within the context of the unique characteristics and risk landscape of the sector.[15] In addition to federal agencies, the National Infrastructure Advisory Council (NIAC) is responsible for providing the President, through the Secretary of Homeland Security, with advice on the security of critical infrastructure sectors and their information systems. NIAC is composed of no more than 30 members, appointed by the President from private industry, academia, and state and local government.[16]

NIST Cyber Framework

In February 2013, then-President Barack Obama issued an Executive Order calling for the development of a voluntary framework to establish common standards for managing cybersecurity risk.[17] Executive Order 13636 of February 12, 2013, "Improving Critical Infrastructure Cybersecurity," directed the Executive Branch to:

- Develop a technology-neutral voluntary cybersecurity framework;
- Promote and incentivize the adoption of cybersecurity practices;

- Increase the volume, timeliness and quality of cyber threat information sharing
- Incorporate strong privacy and civil liberties protections into every initiative to secure U.S. critical infrastructure; and
- Explore the use of existing regulation to promote cyber security.[18]

In response, the National Institute of Standards and Technology (NIST) of the Department of Commerce released the *Framework for Improving Critical Infrastructure Cybersecurity* on February 12, 2014.[19] The NIST Cyber Framework is a voluntary, risk-based framework based on industry standards and best practices to help organizations manage cybersecurity risks.[20] The Framework attempts to provide a common lexicon that can be used across all industries to address and manage cybersecurity risk based on business needs without placing additional regulatory requirements on businesses. The seven steps recommended in the Framework are:

- Step 1: Prioritize and Scope
- Step 2: Orient
- Step 3: Create a Current Profile—A Current Profile provides a baseline for where the organization is today versus where the organization wants to be. The latter is a "Target Profile," discussed below. The Current Profile is the initial step in developing a roadmap towards the Target Profile.
- Step 4: Conduct a Risk Assessment—Risk assessments weigh the impact of an incident, the likelihood or frequency of the incident, and the strength of existing controls.
- Step 5: Create a Target Profile—A Target Profile is where the organization wants to be. While the criteria for developing a target cybersecurity profile varies among organizations and across sectors, the organization should establish objectives that it wants to achieve (e.g., protecting critical systems or data, eliminating known or suspected vulnerabilities in the business environment, and/or complying with a new requirement imposed by contract or law) and develop the Target Profile accordingly.
- Step 6: Determine, Analyze, and Prioritize Gaps in Current and Target Profiles
- Step 7: Develop and Implement an Action Plan—In developing the action plans, organizations take into consideration the most serious risk for potential exposure, the amount of harm they could potentially be exposed to by not acting on the risk, and cost and benefits of the areas for improvement where benefits are the mitigation of risk.[21]

President Trump's May 11, 2017 Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," builds from existing initiatives by requiring federal agencies to adopt the 2014 NIST framework, further establishing a common language and trending toward a duty of care.[22] The Executive Order breaks new ground with potentially industry-altering directives regarding coordination across federal agencies, as well as private sector information-sharing and transparency requirements.[23] Specifically, the Executive Order directs DHS to collaborate with other federal agencies to determine their ability to support the cybersecurity efforts of "section 9 entities," which are a classified group of companies that the U.S. Government has identified as being at the greatest risks of cyber attacks that could result in catastrophic effects on public health, economic security, or national security.[24] The agencies also must examine existing federal policies and practices to determine whether they are sufficient to promote "appropriate market transparency" regarding cybersecurity risk management practices, especially by publicly traded critical infrastructure companies.[25] The Executive Order directs DOD to coordinate an assessment of the risks facing the defense industry.[26] It also directs the Department of Commerce and DHS to jointly lead "an open and transparent process" to reduce automated cyber-attacks,[27] and it directs the Department of Energy to coordinate an assessment of the potential for prolonged power outages associated with cyber incidents.[28]

The Defense Industrial Base

The Defense Industrial Base Sector provides products and services that are essential to mobilize, deploy, and sustain military operations, and includes the design, production, delivery, and maintenance of military weapons systems, subsystems, and components or parts, to meet U.S. military requirements.[29] The DIB Sector consists of both domestic and foreign entities, with production assets located in multiple countries and reportedly includes more than 100,000 companies and their subcontractors.[30]

The 2010 DIB Sector-Specific Plan identifies cybersecu-

rity as the number one threat to the DIB, explaining that this risk flows down the supply chain:

> The DIB relies on commercial-off-the-shelf (COTS) information system products that are often flawed in their design and implementation, thus offering a host of vulnerabilities to those who would exploit them. The vulnerabilities are sometimes significant and other times too subtle to detect easily. In fact, these vulnerabilities are the subject of widespread exploitation efforts by individuals and groups within and outside the U.S.[31]

As such, cybersecurity for the DIB has been a focus in recent years especially as it pertains to cyber incident reporting.

Safeguards

All contractors—not just those in the defense industry—are subject to 15 basic safeguarding requirements under the clause at Federal Acquisition Regulation (FAR) 52.204-21.[32] Under the FAR clause, contractors must protect information systems that process, store, or transmit "Federal contract information" (FCI).[33] FCI is "information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public Web sites) or simple transactional information, such as necessary to process payments."[34] This definition is extraordinarily broad. It includes any information used in the performance of a contract that originated from or will be provided to the Government, apart from information that is public or is "simple transactional information." Contractors should ensure that any system that stores or shares FCI is identified and adequate security controls are in place. These systems are subject to 15 standards—relating to six of the 14 security control "families" in NIST Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations."[35] The FAR rule relating to safeguarding systems with FCI, which was effective June 15, 2016, was in process for more than four years. So presumably contractors with FCI already have taken steps to implement security controls in accordance with the FAR, which should make compliance with all NIST SP 800-171 security controls under the Defense FAR Supplement (DFARS) less onerous.[36]

The more critical and extensive set of controls applicable to DIB contractors are specified by NIST SP 800-171.[37] DOD's final rule for safeguarding "covered defense information" (CDI) requires, under the clause at DFARS 252.204-7012, that defense contractors that process, store, or transmit CDI meet more than 100 security requirements across 14 categories ("families") specified by NIST SP 800-171 "as soon as practical."[38] The definition of CDI in the final rule reads:

> Covered defense information means unclassified controlled technical information or other information (as described in the Controlled Unclassified Information (CUI) Registry at http://www.archives.gov/cui/registry/category-list.html) that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies, and is—
>
> (1) Marked or otherwise identified in the contract, task order or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract; or
>
> (2) Collected, developed, received, transmitted, used or stored by or on behalf of the contractor in support of the performance of the contract.[39]

In response to industry comments, the drafters of the final rule acknowledged that, while there is an "affirmative requirement for Government to mark or otherwise identify in the contract all covered defense information," contractors share an obligation "to recognize and protect covered defense information that the contractor is developing during contract performance."[40] Indeed, "[m]arking media with necessary CUI markings and distribution limitations" is an express security requirement in NIST SP 800-171.[41] Thus, although contractors may rely on their customer to identify CDI, they also must remain vigilant and proactive when it comes to safeguarding CDI.

The deadline for compliance with DFARS 252.204-7012 was December 31, 2017. To the extent contractors are not fully compliant yet, they may face a competitive disadvantage as the final rule "does not preclude a requiring activity from specifically stating in the solicitation that compliance with the NIST SP 800-171 will be used as an evaluation factor in the source selection process."[42] In fact, recent guidance released in September 2017 outlines the ways in which DOD acquisition personnel can leverage the contractor's system security plan (SSP) and any associated plans of action (POA) in the contract formation, administration, and source selection processes. Most notably, DOD reiterates that the buying activity may use the SSP and POA to evaluate the overall risk introduced by the state of the contractor's internal information system/network. Other examples of how the SSP and POA may be used include establishing compliance with DFARS 252.204-7012 as a separate techni-

cal evaluation factor; requiring proposals to (1) identify NIST SP 800-171 security requirements not implemented at the time of award and (2) include associated POA for implementation; and requiring compliance with all NIST SP 800-171 security requirements at the time of award.[43]

Notably, an October 2017 Government Accountability Office (GAO) decision suggests that proposals offering to exceed baseline security requirements may be a distinguishing factor in an award decision. On October 4, 2017, GAO denied a protest by IPKeys Technologies, LLC challenging the Defense Information Systems Agency's (DISA) issuance of a task order to By Light Professional IT Services, Inc. for video services, finding that DISA reasonably assigned a strength to the awardee for exceeding the solicitation's baseline cybersecurity requirement, the Risk Management Framework (RMF), by also showing compliance with the NIST Framework for Improving Critical Infrastructure Cybersecurity.[44] IPKeys argued that DISA's evaluation was unreasonable, unsupported by the facts, and resulted in disparate treatment, in part, because the NIST Framework was either synonymous with or "otherwise subsumed within the RMF." GAO rejected this argument, concluding that the basis of the unique strength awarded was that only By Light voluntarily proposed to incorporate the NIST Framework in addition to the required baseline RMF. While this protest dealt with RMF and the NIST Framework, rather than the requirements under DFARS 252.204-7012, it is instructive to the extent that DFARS 252.204-7012 anticipates contractors will need to exceed baseline requirements (e.g., NIST SP 800-171) where necessary to provide "adequate security," which is broadly defined as "protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information."[45] Therefore, it would be consistent with the plain language of DFARS 252.204-7012 that an agency award a "strength" to a proposal offering to exceed the baseline requirements in NIST SP 800-171 over competing proposals that do not.

Drafters of the DFARS final rule made it clear that compliance with NIST SP 800-171 does not preempt other cybersecurity requirements (or vice versa): "DFARS 204.7300(b) states that the rule 'does not abrogate any other requirements regarding contractor physical, personnel, information, technical, or general administrative security operations governing the protection of unclassified information.' "[46] Although contractors must be mindful of other security obligations, and recognize that compliance with one regime does not necessarily guarantee compliance with others, they still can—and should—leverage documentation and agency guidance under other compliance regimes to support their response to the requirements of NIST SP 800-171.

Stricter standards apply to IT contractors or those that process, store, or transmit Government data. Generally, those contractors must comply with the minimum security requirements in Federal Information Processing Standards (FIPS) Publication 200, "Minimum Security Requirements for Federal Information and Information Systems,"[47] as well as appropriate security controls in NIST SP 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations."[48] The Federal Information Security Management Act (FISMA) requires cloud service providers (CSPs) to implement programs to provide security for information and information systems.[49] The Federal Risk and Authorization Management Program (FedRAMP) provides a standard process for ensuring the security of CSPs for use by the Government.[50] Under the clause at DFARS 252.239-7010, "Cloud Computing Services," CSPs must comply with the Cloud Computing Security Requirements Guide.[51] In contrast, a contractor using an *external* CSP to store or transmit CDI must ensure that the CSP meets security requirements equivalent to those established by the Government for the FedRAMP "moderate" baseline at the time award.[52] The process and resources for securing Government authorization to operate under FedRAMP are well defined and include (1) a readiness assessment phase; (2) an initial authorization phase, which involves creating a system security plan, a security assessment plan, a security assessment report, a plan of action, and milestones; and (3) a continuous monitoring phase.[53] Resources and a security assessment framework are available for both low and moderate impact level systems, which are subject to different control levels under NIST SP 800-53.

Cyber Incident Reporting

The final rule on the DOD's DIB Cybersecurity (CS) Activities implements statutory requirements for DOD contractors and subcontractors to report cyber incidents within 72 hours that result in an actual or potentially adverse effect on a covered contractor information system or CDI residing therein or on a contractor's ability to provide operationally critical support.[54] The mandatory reporting applies to all forms of agreements between DOD and DIB companies (contracts, grants, cooperative agreements, other transaction agreements, technology investment agreements, and any other type of legal instrument or agreement).[55] Sim-

ilar to the requirements for other sectors, cybersecurity safeguards and reporting requirements are triggered by the data. Therefore, safeguards and cyber incident reporting involving classified information on classified contractor systems must be in accordance with the National Industrial Security Program Operating Manual.[56] The table below identifies other reporting mechanisms of which contractors should be aware.

Organization		What to Report?
U.S. Department of Homeland Security (DHS)	National Protection and Programs Directorate (NPPD), National Cybersecurity and Communications Integration Center (NCCIC)	Suspected or confirmed cyber incidents that may impact critical infrastructure and require technical response and mitigation assistance
	U.S. Secret Service	Cybercrime, including computer intrusions or attacks, transmission of malicious code, password trafficking, or theft of payment card or other financial payment information
	U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI)	Cyber-based domestic or international cross-border crime, including child exploitation, money laundering, smuggling, and violations of intellectual property rights
U.S. Department of Justice (DOJ)	Federal Bureau of Investigation	Cybercrime, including computer intrusions or attacks, fraud, intellectual property theft, identity theft, theft of trade secrets, criminal hacking, terrorist activity, espionage, sabotage, or other foreign intelligence activity

Mandatory Flow-Down Provisions

Both the FAR and DFARS safeguarding rules include a flow-down requirement. FAR 52.204-21(c) requires the contractor to "include the substance of this clause, including this paragraph (c), in subcontracts under this contract (including subcontracts for the acquisition of commercial items, other than commercially available off-the-shelf items [COTS]), in which the subcontractor may have Federal contract information residing in or transiting through its information system." Thus, with the exclusion of COTS suppliers, all subcontractors will be subject to the same rules as their prime contractors whenever the subcontractor will handle federal contract information (FCI).

DFARS 252.204-7012(m) requires the contractor to flow down the clause if a subcontractor will handle CDI or if a subcontract is for "operationally critical support," which is defined as "supplies or services designated by the government as critical for airlift, sealift, intermodal transportation services, or logistical support that is essential to the mobilization, deployment, or sustainment of the Armed Forces in a contingency operation."[57] DOD's answers to industry questions clarify that the contractor "should" consult with the CO to determine whether the subcontract will involve CDI and will require flow-down of the clause.[58] DOD also clarified that the clause is not required in contracts solely for COTS items, but it did not address specifically the applicability to subcontracts involving only COTS items.[59] Thus, it is possible the clause would be required to be flowed down to a subcontractor providing only COTS items if the prime contract is not solely for COTS items.

Additionally, all DOD contracts for information technology involving a "national security system" are required to manage supply chain risk under the clause at DFARS 252.239-7018. "Supply chain risk" is defined as "the risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a national security system (as that term is defined at 44 U.S.C. 3542(b)) so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system."[60] The clause is not specific as to the actions a prime contractor must take to mitigate supply chain risk. However, if a contractor flows down all of the cybersecurity requirements pursuant to FAR 52.204-21 and DFARS 252.204-7012, it is unclear what more is needed.

Risk Mitigation

Risks abound for government contractors operating in the critical infrastructure sphere—including but not limited to civil and criminal liability, terminations for default, and lost business reputation. However, there are a few ways in which contractors can mitigate that risk.

Protected Critical Infrastructure Information (PCII) Program

Certain contractors may apply for the safe harbor provisions if they hold a select subset of CII—known as Protected Critical Infrastructure Information (PCII). PCII is protected from disclosure under the federal Freedom of Information Act (FOIA),[61] as well as state and local equivalents to FOIA, and from use in civil litigation or for regulatory purposes.[62] To qualify for these protections, organizations must first

voluntarily submit their information to the Federal Government under the PCII Program, whose purpose is to promote the free exchange of information between the private and public sector for the purposes of homeland security.[63] Other advantages of the PCII program include oversight to ensure uniform procedures are in place for the receipt, validation, handling, storage, marking, and use of PCII, including taking reasonable steps to ensure that the individuals follow PCII safeguarding policies and procedures.[64] Additionally, violations of the PCII Program procedures may result in either criminal or administrative penalties.[65]

The SAFETY Act

The Support Anti-terrorism by Fostering Effective Technologies (SAFETY) Act offers another risk mitigation tool defense contractors should consider.[66] As part of the Homeland Security Act of 2002, Public Law 107-296, Congress enacted liability protections for providers of certain anti-terrorism technologies.[67] The SAFETY Act provides incentives for the development and deployment of anti-terrorism technologies by creating a system of ''risk management''[68] and a system of ''litigation management.''[69] The purpose of the Act is to ensure that the threat of liability does not deter potential manufacturers or sellers of anti-terrorism technologies from developing, deploying, and commercializing technologies that could save lives. Under the SAFETY Act, contractors may receive certain liability limitations for ''claims arising out of, relating to, or resulting from an act of terrorism'' where Qualified Anti-Terrorism Technologies (QATTs) are implicated.

Under FAR Subpart 50.2, which implements the SAFETY Act, an "act of terrorism" means—

> any act determined to have met the following requirements or such other requirements as defined and specified by the Secretary of Homeland Security:
>
> (1) Is unlawful.
>
> (2) Causes harm, including financial harm, to a person, property, or entity, in the United States, or in the case of a domestic United States air carrier or a United States-flag vessel (or a vessel based principally in the United States on which United States income tax is paid and whose insurance coverage is subject to regulation in the United States), in or outside the United States.
>
> (3) 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.[70]

FAR Subpart 50.2 defines a QATT as "any technology designed, developed, modified, procured, or sold for the purpose of preventing, detecting, identifying, or deterring acts of terrorism or limiting the harm such acts might otherwise cause, for which a SAFETY Act designation has been issued.[71] A QATT "technology" means "any product, equipment, service (including support services), device, or technology (including information technology) or any combination of the foregoing. Design services, consulting services, engineering services, software development services, software integration services, threat assessments, vulnerability studies, and other analyses relevant to homeland security may be deemed a technology."[72] Thus, the SAFETY Act "approved" technologies are broadly defined. QATT technologies identified by DHS listed in a 2007 Federal Acquisition Circular amending the FAR included vulnerability assessment and countermeasure and counter-terrorism planning tools; first responder interoperability solution; marine traffic management system; security services, guidelines, systems, and standards; vehicle and cargo inspection system; X-ray inspection system; trace explosives detection systems and associated support services; maintenance and repair of screening equipment; risk assessment platform; explosive and weapon detection equipment and services; biological detection and filtration systems; passenger screening services; baggage screening services; chemical, biological, or radiological agent release detectors; vehicle barriers; first responder equipment; and architectural and engineering "hardening" products and services.[73] However, DHS's current SAFETY Act database indicates that the technologies and the companies that are covered under the SAFETY Act run cross-industry and cover not only the technology's hardware and software but also the site support services and labor associated with the technology, such as project management, analytics, training, and systems engineering and integration services for the design, development, and deployment of the technology.[74]

The SAFETY Act "approvals" are generally two-tiered. A "SAFETY Act designation" means DHS determined, pursuant to 6 U.S.C.A. § 441 (b) and 6 U.S.C.A. § 443(a), as further delineated in the DHS regulations, 6 C.F.R. § 25.4, that a particular technology constitutes a QATT under the SAFETY Act.[75] Technologies that receive a SAFETY Act designation are eligible for a "SAFETY Act certification," which means DHS determined, pursuant to 6 U.S.C.A. § 442(d), as further delineated in 6 C.F.R. §§ 25.8 and 25.9, that the QATT "is an approved product for homeland security, *i.e.*, it will perform as intended, conforms to the seller's specifications, and is safe for use as intended."[76] DHS may

also issue a "block certification" or a "block designation" for a "technology class."[77] Prior to bidding on a solicitation, contractors should check if the solicitation notifies offerors that the technology to be procured either affirmatively or presumptively satisfies the technical criteria necessary to be deemed a QATT. If there is this language—known as a "pre-qualification designation notice"[78]—then offerors are authorized to submit streamlined SAFETY Act applications for SAFETY Act designation and receive expedited processing of those applications.[79]

Cyber Due Diligence

Companies considering bidding on a contract in a new critical infrastructure sector or with a new agency should first assess whether there are cybersecurity risks implicated as part of the capture team's business case. This might require not only a cyber-risk assessment of the contracting agency and designated Sector-Specific Agency, but also any vendors, teammates, or subcontractors. Failure to take these steps could result in dramatically underbidding the work, including the cost of compliance. More importantly, some of the most high-profile data breaches in recent years have been linked to data security vulnerabilities from third-party vendors. While it remains unclear the extent to which a contractor will be liable for the actions or inactions of subcontractors, suppliers, and third-party vendors following a data breach, contractors would be unwise to assume that third-party cybersecurity issues are not their issues as well. To the contrary, DOD guidance suggests that contractors will be responsible, at least in some instances, for the noncompliance of their subcontractors and CSPs.[80] Thus, basic knowledge of the capabilities and vulnerabilities of subcontractors, partners and teammates, as well as an understanding of each party's cybersecurity obligations under their contracts with each other, are vital.

Before entering into a joint venture or teaming agreement, contractors should conduct a due diligence into cybersecurity risks presented by potential teammates. Assessing the potential impact and downstream costs if those risks materialize allows the capture team to more accurately assess the value of the prospective business relationship, which in turn garners an upper hand in negotiations. Admittedly, reaching agreement on a cyber due diligence may have challenges where there is unequal bargaining power between the two parties. The agreement should cover management buy-in, provide for appropriate stakeholder involvement, and address what documents will need to be shared by the parties. Where available, the potential partner should provide the contractor with documentation that supports its responses. For example, contractors should examine one another's privacy policies, business continuity and disaster recovery plans, audit documentation, and insurance coverage. Below is a checklist of basic due diligence considerations contractors should cover.

- *Data:* Cybersecurity requirements, such as safeguards and incident reporting, depend upon the specific contracts and the types of information that is stored, processed, or accessed by the contractor.
    1. What type of data will be shared/accessed/stored/maintained?
    2. Who are the data custodians?
    3. How is the data classified?
    4. What are the applicable statutory and regulatory requirements for the data? Are there any additional requirements to protect the data, including those imposed by the company's contracts with other parties or customers?
    5. Where is the data stored? Does the company have its data backed up somewhere where it can be recovered quickly to resume business?
- *Security:*
    1. What, if any, security measures are in place to safeguard customer data?
    2. What, if any, electronic measures are in place to safeguard the data (*e.g.*, firewalls)?
    3. Does the company regularly assess those security measures for vulnerability? If so, how frequently?
- *Plans, Policies, and Procedures:*
    1. Does the company have data-handling processes in place to ensure compliance with applicable laws?
    2. Does the company have privacy policies and procedures in place that employees and its other vendors are required to follow?
    3. What, if any, policies are in place to safeguard the data?
    4. Does the company have a plan for disaster recov-

ery and business continuity in the event of an outage?

5. Does the company monitor and assess employee and other third-party company compliance with these plans, policies, and procedures? If so, how frequently?

- *Data Breaches and Liability Concerns:*

1. Has an unauthorized party ever attempted to infiltrate the company's system? If so, describe the quantity and type of data compromised, date of the incident, date of resolution, and how the incident was resolved.

2. Has the company experienced any data security breaches that affected its business? If so, describe the quantity and type of data compromised, date of the incident, date of resolution, and how the incident was resolved.

3. Is the company pursuing a claim against the person(s) responsible for the incident? Hacker(s)?

4. Is there any pending or threatened litigation related to the company's handling of sensitive data or a breach to its data security? Have any claims *ever* been brought against the company related to its handling of sensitive data or a breach to its data security? If so, when and what was the outcome of that litigation?

5. Is there any pending or threatened government investigation related to the company's handling of sensitive data? Has the government *ever* investigated the company for mishandling customer data? If so, when and what was the outcome of that investigation?

- *Representations and Warranties:*

1. The company should certify that all information provided during the due diligence investigation was truthful and complete.

2. The company should certify that it is currently compliant and will remain compliant with all applicable state and federal data privacy laws, including notification laws in the event of a breach.

Guidelines

These *Guidelines* suggest some key considerations for managing cybersecurity in the U.S. Defense Industrial Base. They are not, however, a substitute for professional representation in any specific situation.

1. Be aware that cybersecurity requirements, such as safeguards and incident reporting, depend upon the specific contracts and the types of information that is stored, processed, or accessed by the contractor.

2. Be aware that, while the Government has a duty to mark or identify all covered defense information under DFARS 252.204-7012, contractors share an obligation to identify, mark, and protect covered defense information that the contractor develops during contract performance.

3. DOD acquisition personnel may leverage the contractor's system security plan and any associated plans of action in the contract formation, administration, and source selection processes.

4. Contractors may avoid reinventing the wheel by leveraging documentation and guidance under other compliance regimes to support responses to the DFARS requirements.

5. Contractors may mitigate their liability risk by applying to participate in the PCII Program or receiving a SAFETY Act approval.

6. Before entering into a joint venture or teaming agreement, contractors should conduct a due diligence into cybersecurity risks presented by potential teammates to ensure that the potential teammate will not introduce vulnerabilities in the system and to assess potential downstream liability.

ENDNOTES:

[1]"The United States (U.S.) National Security Strategy" at 12 (Dec. 2017), https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf ("For most of our history, the United States has been able to protect the homeland by controlling its land, air, space, and maritime domains. Today, cyberspace offers state and non-state actors the ability to wage campaigns against American political, economic, and security interests without ever physically crossing our borders. Cyberattacks offer adversaries low-cost and deniable opportunities to seriously damage or disrupt critical infrastructure, cripple American businesses, weaken our Federal networks, and attack the tools

and devices that Americans use every day to communicate and conduct business. . . . The vulnerability of U.S. critical infrastructure to cyber, physical, and electromagnetic attacks means that adversaries could disrupt military command and control, banking and financial operations, the electrical grid, and means of communication."); see also Tadeo, "Nation-State Cyber Attacks Come Out of the Shadows," NS Tech (Apr. 12, 2017), http://tech.newstatesman.com/guest-opinion/nation-state-cyber-attacks-come-shadows.

[2]42 U.S.C.A. § 5195c(e).

[3]The sectors are identified in Presidential Policy Directive—Critical Infrastructure Security and Resilience, PPD-21 (Feb. 12, 2013), https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil; see https://www.dhs.gov/critical-infrastructure-sectors.

[4]Press Release, New Lloyd's Study Highlights Wide Ranging Implications of Cyber Attacks (July 8, 2015), https://www.lloyds.com/news-and-insight/press-centre/press-releases/2015/07/business-blackout.

[5]See Dep't of Transp. (DOT), Nat'l Highway Traffic Safety Admin., "Nat'l Institute of Standards and Technology Cybersecurity Risk Management Framework Applied to Modern Vehicles," DOT HS 812 (Sept. 2014); see also DOT, Nat'l Highway Traffic Safety Admin., "Cybersecurity Best Practices for Modern Vehicles," DOT HS 812 333 (Oct. 2016).

[6]Rainie & Maniam, "Americans Feel the Tensions Between Privacy and Security Concerns," Fact Tank, Pew Research Center (Feb. 19, 2017), http://www.pewresearch.org/fact-tank/2016/02/19/americans-feel-the-tensions-between-privacy-and-security-concerns/.

[7]See Verizon, 2017 Data Breach Investigations Report 28–29 (10th ed.), available at http://www.verizonenterprise.com/resources/reports/rp_DBIR_2017_Report_en_xg.pdf [hereinafter "2017 Verizon Report"]. The 2017 Verizon Report defines "cyber-espionage" to include "unauthorized network or system access linked to state-affiliated actors and/or exhibiting the motive of espionage." 2017 Verizon Report at 42–43. Incidents tagged as "misuse" are defined as "any unapproved or malicious use of organizational resources. . . . This is mainly insider-only misuse, but outsiders (due to collusion) and partners (because they are granted privileges) show up as well." 2017 Verizon Report at 48–49.

[8]2017 Verizon Report at 28–29 (citing "state-affiliated" as the leading cause of confirmed data breaches).

[9]See https://www.symantec.com/theme.jsp?themeid=apt-infographic-1; see, e.g., Greenberg, "New Group of Iranian Hackers Linked to Destructive Malware," Wired (Sept. 20, 2017), https://www.wired.com/story/iran-hackers-apt33/ (discussing link between APT-33 and Iran); Testimony of Frank J. Cilluffo, Dir., Center for Cyber & Homeland Security, on Emerging Cyber Threats to the United States Before the H. Comm. on Homeland Security Subcomm. on Cybersecurity, Infrastructure Protection, and Security Technologies 2 (Feb. 25, 2016), available at http://docs.house.gov/meetings/HM/HM08/20160225/104505/HHRG-114-HM08-WstateCilluffoF-20160225.pdf (explaining that "[n]ation-states and their proxies continue to present the greatest—meaning most advanced and persistent—threat in the cyber domain. . . . Nation-states often use proxies to conceal state involvement. In turn, there are different grades of proxies: they may be state-sanctioned, state-sponsored, or state-supported.").

[10]See Connell & Vogler, Russia's Approach to Cyber Warfare (CNA Mar. 2017), available at https://www.cna.org/CNA_files/PDF/DOP-2016-U-014231-1Rev.pdf; see also North Korea's Cyber Capabilities, Center for Strategic & International Studies, https://www.csis.org/programs/korea-chair/korea-chair-project-archive/north-koreas-cyber-capabilities.

[11]Connell & Vogler, Russia's Approach to Cyber Warfare 3 & n.4 (CNA Mar. 2017), available at https://www.cna.org/CNA_files/PDF/DOP-2016-U-014231-1Rev.pdf ("According to the Military Doctrine of the Russian Federation (2010), one of the features of modern military conflicts is 'the prior implementation of measures of information warfare in order to achieve political objectives without the utilization of military force and, subsequently, in the interest of shaping a favourable response from the world community to the utilization of military force.' ").

[12]See, e.g., Greenberg, " 'Crash Override': The Malware That Took Down a Power Grid," Wired (June 12, 2017), https://www.wired.com/story/crash-override-malware/ (Ukraine); Corera, "How France's TV5 Was Almost Destroyed by 'Russian Hackers,' " BBC News (Oct. 10, 2016), http://www.bbc.com/news/technology-37590375.

[13]Taddeo, "Nation-State Cyber Attacks Come Out of the Shadows," NS Tech (Apr. 12, 2017), http://tech.newstatesman.com/guest-opinion/nation-state-cyber-attacks-come-shadows.

[14]See https://www.dhs.gov/sector-specific-agencies.

[15]DHS, National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience app. B, available at https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf.

[16]See https://www.dhs.gov/national-infrastructure-advisory-council.

[17]Exec. Order No. 13636, 78 Fed. Reg. 11739 (Feb. 19, 2013).

[18]Exec. Order No. 13636, 78 Fed. Reg. 11739 (Feb. 19, 2013).

[19]NIST, Framework for Improving Critical Infrastructure Cybersecurity (Feb. 12, 2014), available at http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

[20]See also NIST, Framework for Improving Critical Infrastructure Cybersecurity, Draft Version 1.1 (tracking changes between 2014 ver. and ver. 1.1, Jan. 10, 2017), available at https://www.nist.gov/sites/default/files/documents////draft-cybersecurity-framework-v1.1-with-markup1.pdf. The 2017 draft Framework incorporates feedback since the release of Framework Version 1.0 and integrates com-

ments from the December 2015 Request for Information as well as comments from attendees at the Cybersecurity Framework Workshop 2016 held at the NIST campus in Gaithersburg, Maryland.

[21]NIST, Framework for Improving Critical Infrastructure Cybersecurity 14 (Feb. 12, 2014), available at http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

[22]Exec. Order No. 13800, 82 Fed. Reg. 22391 (May 16, 2017).

[23]Exec. Order No. 13800, 82 Fed. Reg. 22391 (May 16, 2017).

[24]Exec. Order No. 13800, § 2(b), 82 Fed. Reg. 22391, 22393 (May 16, 2017); see Exec. Order No. 13636, § 9, 78 Fed. Reg. 11739, 11742 (Feb. 19, 2013).

[25]Exec. Order No. 13800, § 2(c), 82 Fed. Reg. 22391, 22394 (May 16, 2017).

[26]Exec. Order No. 13800, § 2(f), 82 Fed. Reg. 22391, 22394 (May 16, 2017). Initially, DOD planned to survey hundreds of companies to identify weaknesses, which was seen as burdensome for defense contractors. In December 2017, however, it was announced that the survey process was halted until DOD could coordinate with data previously collected by the Office of Management and Budget.

[27]Exec. Order No. 13800, § 2(d), 82 Fed. Reg. 22391, 22394 (May 16, 2017).

[28]Exec. Order No. 13800, § 2(e), 82 Fed. Reg. 22391, 22394 (May 16, 2017).

[29]DHS, The Defense Industrial Base, https://www.dhs.gov/defense-industrial-base-sector.

[30]DHS, The Defense Industrial Base, https://www.dhs.gov/defense-industrial-base-sector.

[31]DHS & DOD, Defense Industrial Base Sector-Specific Plan 2010, at 33 (May 2010), available at https://www.dhs.gov/sites/default/files/publications/nipp-ssp-defense-industrial-base-2010-508.pdf.

[32]FAR 52.204-21(b).

[33]FAR 52.204-21(b)(1).

[34]FAR 52.204-21(a).

[35]See FAR 52.204-21(b)(1)(i)–(xv); NIST SP 800-171, Rev. 1, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations," at 9-15 (Dec. 2016), available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf; see also Draft NIST SP 800-171A, Assessing Security Requirements for Controlled Unclassified Information (Nov. 2017), available at https://csrc.nist.gov/CSRC/media/Publications/sp/800-171a/draft/sp800-171A-draft.pdf).

[36]See DFARS 252.204-7012.

[37]NIST SP 800-171, Rev. 1 (Dec. 2016).

[38]81 Fed. Reg. 72986 (Oct. 21, 2016); DFARS 252.204-7012(b)(2)(ii)(A). The deadline for compliance was December 31, 2017.

[39]DFARS 252.204-7009(a).

[40]81 Fed. Reg. at 72988 (responding to comments seeking clarification on the definition of CDI, with several contractors hoping this information could be limited to that specifically designated by the Government under a contract).

[41]NIST SP 800-171, Rev. 1, 3.8.4 (Dec. 2016).

[42]81 Fed. Reg. at 72990.

[43]Memorandum from Shay D. Assad, Dir., Defense Pricing/Defense Procurement & Acquisition Policy, "Implementation of DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting" (Sept. 21, 2017), available at http://dodprocurementtoolbox.com/cms/sites/default/files/resources/2017-09/USA002829-17-DPAP.pdf.

[44]IPKeys Techs., LLC, Comp. Gen. Dec. B-414890 et al., 2017 CPD ¶ 311, 2017 WL 5235092.

[45]DFARS 252.204-7012(a).

[46]81 Fed. Reg. at 72987.

[47]FIPS Pub 200, "Minimum Security Requirements for Federal Information and Information Systems" (Mar. 2006), available at http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf.

[48]NIST SP 800-53, Rev. 4, "Security and Privacy Controls for Federal Information Systems and Organizations" (Apr. 2013), available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

[49]44 U.S.C.A. §§ 3551–3558.

[50]See https://www.fedramp.gov.

[51]DFARS 252.239-7010(b)(1); see https://iase.disa.mil/cloud_security/Pages/index.aspx.

[52]DFARS 252.204-7012(b)(2)(ii)(D); see 81 Fed. Reg. 72994.

[53]See https://www.fedramp.gov/resources/templates-2016/.

[54]81 Fed. Reg. 68312 (Oct. 4, 2016) (amending 32 C.F.R. pt. 236).

[55]32 C.F.R. § 236.4.

[56]32 C.F.R. § 236.5; see National Industrial Security Program Operating Manual, DOD 5220.22-M (Feb. 28, 2006), incorporating Change 2 (Mar. 18, 2016), available at http://dtic.mil/whs/directives/corres/pdf/522022M.pdf.

[57]DFARS 252.204-7012(a).

[58]See DOD FAQs Regarding Network Penetration Reporting and Contracting for Cloud Services (DFARS Case 2013-D018), DFARS subpt. 204.73 and Procedures, Guidance and Information subpt. 204.73, and DFARS subpt. 239.76 and PGI subpt. 239.76, FAQ No. 5 (Jan. 27, 2017), available at https://www.acq.osd.mil/dpap/pdi/docs/FAQs_Network_Penetration_Reporting_and_Contracting_for_Cloud_Services_(01-27-2017).pdf [hereinafter DOD FAQs].

[59]See DOD FAQs, FAQ No. 3; 81 Fed. Reg. 72986, 72987 (Oct. 21, 2016) (prescriptions at DFARS 204.7304 for use of DFARS clause exclude COTS contracts).

[60]DFARS 252.239-7018(a).

[61]5 U.S.C.A. § 552.

[62]See Critical Infrastructure Information (CII) Act of 2002, 6 U.S.C.A. §§ 131–134; 6 C.F.R. pt. 29. Critical Infrastructure Information (CII) is defined under § 212(3) of the Homeland Security Act of 2002 to include information not customarily in the public domain and related to the security of critical infrastructure or protected systems. 6 U.S.C.A. § 131(3).

[63]See 6 C.F.R. pt. 29; https://www.dhs.gov/pcii-program.

[64]See 6 C.F.R. pt. 29.

[65]Violations under Title 18 may result in an individual being fined up to $250,000; imprisoned up to one year; fined and imprisoned; or removed from office or employment. See 6 C.F.R. § 29.9.

[66]Homeland Security Act of 2002, Pub. L. No. 107-296, §§ 861–865 (codified at 6 U.S.C.A. §§ 441–444).

[67]Additional information on the SAFETY Act can be found at the DHS website, https://www.safetyact.gov/. Ensuring that a company has adequate insurance coverage is a prerequisite for obtaining any limits on liability under the SAFETY Act. See 6 U.S.C.A. § 443.

[68]See 6 U.S.C.A. § 443.

[69]See 6 U.S.C.A. § 442.

[70]FAR 50.201.

[71]FAR 50.201.

[72]FAR 50.201.

[73]See FAC 2005-21, Item 1, 72 Fed. Reg. 63026 (Nov. 7, 2007).

[74]See DHS, List of Approved Technologies, https://www.safetyact.gov/lit/at/aa.

[75]FAR 50.201.

[76]FAR 50.201.

[77]See FAR 50.201; 6 C.F.R. §§ 25.6(h), 25.9(j). Block designations and block certifications granted by DHS are include on the DHS website, https://www.safetyact.gov/.

[78]FAR 50.201.

[79]See FAR 50.205-2.

[80]See, e.g., DOD Cloud Computing Security Requirements Guide, Version 1, Release 3 (Mar. 6, 2017, https://iasecontent.disa.mil/cloud/SRG/index.html ("While the CSP's overall service offering may be inheriting controls and compliance from a third party, the prime CSP, the CSP with a DoD contract for service, is ultimately responsible for complete compliance. This applicability statement and associated requirements are consistent with DoD and Federal acquisition requirements and clauses which state that DoD contractors, in this case integrators/brokers/CSPs must include all security requirements incumbent upon them in all subcontracts.").

NOTES:

NOTES:

BRIEFING PAPERS