CYBER RISK:
Navigating the Rising Tide of Cybersecurity Regulation
With hacking and other “cyber incidents” now growing by nearly 40% every year, governments around the world are taking an increasingly active role in defining new requirements for corporate information security. They are passing new legislation, adopting new regulations, and tightening up procurement contracts. Case in point: During the past three years in the U.S., more than 240 bills, amendments and other legislative proposals have been introduced in Congress seeking to regulate, allocate funding to, or otherwise address various aspects of cybersecurity.

Governments also are working with the private sector on new voluntary standards and best practices designed to achieve stronger cybersecurity protections and to safeguard confidential information from loss and theft.

The diversity and complexity of cybersecurity risks, and their evolving character, have caused governments to respond in many different ways. They have been motivated by a variety of policy concerns: protecting individuals’ sensitive personal, health and financial information; safeguarding companies’ proprietary data and competitiveness; and defending critical infrastructure and national security.

Some governments are taking action directly to require the cybersecurity of various public and private networks and systems. Others are encouraging the development of voluntary frameworks and best practices that industries can choose to adopt. Some have adopted new requirements that are fairly general, while some actions are both specific to the protection objectives and prescriptive to the measures required. Some require information security with respect to particular kinds of data, while others deal with cybersecurity for all kinds of company data. Some of these requirements are being mandated by specific government legislation, while others are being implemented by regulatory agencies or as the result of agency or law enforcement actions, or private lawsuits.

Government efforts to defend against cyber threats are, in short, a patchwork. While there is common appreciation of cyber risks, at least at a high level, there is little coherence to these efforts, even within national borders, and even less coordination internationally. Most troubling for businesses trying to find an operational footing in this important area, these new requirements are often inconsistent among different governments, between different agencies of the same government, and from industry to industry. Sector-specific guidelines and standards are proliferating in the transaction processing, financial services, health care and other fields. One of the major unknowns for companies is whether they can embrace one overall information security framework, or whether they will face a splintered environment with an unmanageable number of different corporate, industry and government requirements, standards and practices.

This whitepaper surveys key legislative, regulatory and court-imposed cybersecurity developments that will impact the private sector and governments. It provides an overview of the efforts that governments are undertaking to expand cybersecurity requirements through regulation and procurement actions. It also reviews the development and utilization of the voluntary Framework for Improving Critical Infrastructure Cybersecurity (the “NIST Framework”), developed by the National Institute of Standards and Technology (“NIST”) unit of the U.S. Department of Commerce, and other information-protection standards where NIST has shown leadership.

Finally, this paper highlights the importance of companies and governments taking a broad risk-based, management-systems approach as they work to improve their cybersecurity programs. It promotes leveraging a common cybersecurity framework—such as the NIST Framework—to guide sector-specific voluntary actions and inform nations and companies of useful strategies and methods that can evolve as the threat landscape changes, and can support regulation or even enforcement in critical areas. Indeed, the NIST Framework provides the opportunity to bring some cohesion to the disparate cybersecurity efforts and requirements that have been developing to date.
# TABLE OF CONTENTS

Overview

I. New and Expanded Cybersecurity Regulation

II. Tightened Government Contracting Requirements

III. Growing Use and Importance of Cybersecurity Frameworks and Standards

IV. Implementing Leading Practices

References
An estimated 79% of companies have experienced cyber incidents in the past year. As cybersecurity threats have grown in their severity and pervasiveness, information security has become a leading priority for organizations and governments worldwide.

This whitepaper examines the wave of new legislation, regulations, procurement requirements, and court-imposed developments that are following the dramatic increase in hacking and cybersecurity incidents.

This whitepaper also explores new voluntary standards and best practices that are being developed in collaboration between governments and the private sector to achieve stronger cybersecurity protections and to safeguard confidential information from theft and loss. Specifically reviewed is the development and growing use of the U.S. National Institute of Standards and Technology's voluntary Framework for Improving Critical Infrastructure Cybersecurity (the “NIST Framework”).

In light of the current risk landscape, it is vital for companies and governments to integrate cyber risk into their enterprise-wide risk management. Use of a common risk management program, such as the NIST Framework, provides the opportunity to bring some consistency and cost-effectiveness to the varying cybersecurity efforts and requirements that have been developing to date. Such an approach can help companies and other organizations assess, manage, and respond to their particular cyber risks more effectively, whether they are small or large enterprises.

The Center for Responsible Enterprise and Trade (CREATe.org) has produced this whitepaper to offer insights into the growing trend of cybersecurity regulation, and to help provide practical guidance to companies and governments seeking to proactively manage cyber risks and implement information security.

May 2016

FOR MORE INFORMATION
Please visit www.CREATe.org, via email at info@create.org or follow us on Twitter @CREATe_org.

Companies having cyber incidents in the past year: 79%

Increase in the number of cyber incidents: 38%

Companies having more than $10M in losses from cyber incidents: 10%

PwC
More than 240 bills, amendments and other legislative proposals dealing with cybersecurity have been introduced in the U.S. Congress in the past three years.
While there may be some shortcomings to the NIST Framework—such as specifics around supply-chain management—the alternative is not attractive. Already, there is evidence of a multitude of separate initiatives by standards setting organizations. Some of these may be useful in particular ways. But the risk is all too real that the panoply of discrete, separately developed standards will produce chaotic results, in particular, inconsistencies among standards and confusion among those who are intended to benefit. Pursuit of a common framework approach, particularly as outlined in the NIST Framework, would seem much preferable to the splintered result of hundreds of differing corporate, industry and government standards and practices within the U.S. and globally.

For companies and governments concerned about cybersecurity and compliance, this paper provides vital insights into key regulatory trends, standards and recommendations. It also leverages CREATe.org’s global experience working with companies on the protection of critical corporate information assets to offer guidance about how to improve protections and, at the same time, prepare for the rising tide of cybersecurity regulation.

### I. NEW AND EXPANDED CYBERSECURITY REGULATION

Governments are imposing new and tighter laws and regulations requiring companies and other organizations to implement cybersecurity controls. These range from obligations mandated directly by governments, both for their own data and for industry sectors deemed “critical infrastructure,” to legal requirements to protect particular kinds of confidential information, such as personal data, in specific ways. Other regulatory areas, such as securities and unfair competition, are also expanding their mandates to require cybersecurity as a key aspect of corporate compliance.

#### A. DIRECT REQUIREMENTS TO IMPLEMENT CYBERSECURITY PROTECTIONS

Governments around the world have adopted or are considering legislation that would specifically impose cybersecurity requirements on industry in various ways, particularly in “critical infrastructure” sectors.

In the U.S., although the announced view so far has been that “cyber protection should be the product of self-interest and market forces – not a response to federal dictates,” specific requirements for information security safeguards have already been imposed on the financial services and health care sectors. New legislation appearing in Europe and Asia likewise will impose cybersecurity expectations on a significant range of private-sector industries.

The shared view among governments and industry is that cybersecurity is an important and growing problem, and that many existing practices are inadequate or inconsistent. But despite what individual companies may be doing to mitigate their own risks, for governments in the U.S. and other parts of the world, the perceived threat to information-based economies means that more regulation will be coming. At the same time, many companies and trade associations continue to advocate that governments refrain from using statutes or regulation to require cybersecurity measures.

#### 1. CYBERSECURITY REQUIREMENTS IN CRITICAL INFRASTRUCTURE SECTORS

**U.S.** Specific regulation imposing information security requirements in the private sector appeared first in the financial and health care sectors. While this regulation initially was motivated by a desire to protect individuals’ interests in their sensitive financial and health information, the financial, health care and other fields have also been subsequently identified by the U.S. government as part of the nation’s “critical infrastructure … vital to public confidence and the nation’s safety, prosperity and well-being.” The relevant legal rules are thus evolving from mandates simply to protect individuals’ interests in their data to affirmative cybersecurity management requirements that also protect critical infrastructure in these sectors.

The Gramm-Leach-Bliley Act of 1999 (“GLBA”) governs information sharing practices and safeguards for sensitive
customer data among companies that offer financial or investment advice, loans or insurance. The Safeguards Rule adopted by the Federal Trade Commission (“FTC”) under this Act three years later requires covered institutions to “develop, implement, and maintain a comprehensive written information security program that contains administrative, technical, and physical safeguards” appropriate to the entity, its relevant activities and its customer data.

The Safeguards Rule specifies that covered companies must take five steps in developing their information security programs:

- Designate an employee or employees to coordinate the safeguards;
- Identify and assess the risks to customer information in each relevant area of the company’s operation, and evaluate the effectiveness of current safeguards for controlling these risks;
- Design a safeguards program, and detail the plans to monitor it;
- Select appropriate service providers and require them (by contract) to implement the safeguards; and
- Evaluate the program and explain adjustments in light of changes to its business arrangements or the results of its security tests.

The rule also requires that institutions consider at least three areas of operation in their risk assessments:

- Employee training and management;
- Information systems, including network and software design, and information processing, storage, transmission and retrieval; and
- Security management, including prevention, detection and response to attacks, intrusions or other system failures.

Similar requirements have been imposed on the U.S. health care sector under the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”). HIPAA directed the Department of Health and Human Services (“HHS”) to develop standards and procedures for protecting individuals’ health data more effectively among health care providers, health plans and health clearinghouses that transmit the information in electronic form.

The Security Rule adopted by HHS to implement these requirements mandates that covered entities ensure the confidentiality, integrity and availability of data that they create, receive, maintain or transmit in electronic form; identify and protect against reasonably anticipated threats to the security or integrity of the information; protect against reasonably anticipated, impermissible uses or disclosures; and ensure compliance by their workforce.

This framework requires implementation of a number of administrative, physical and technical safeguards. Covered companies must—in a variety of ways specified by the regulation—conduct risk assessment and risk management; implement administrative, physical and technical safeguards; maintain appropriate policies, procedures and records; address organizational requirements such as reporting and dealing with breaches; and conduct ongoing reviews.

To date HHS has already investigated and resolved more than 24,000 enforcement cases against health sector entities and their business associates for noncompliance with these rules. Thirty-one cases involving digital as well as physical breaches have been settled for a combined value of nearly $28 million. Recently action was taken against a health plan whose stolen computer hard drives contained one million individuals’ health patient records.

European Union (EU) NIS Directive. Long considered a leader in requiring companies to protect individuals’ personal data, the European Union is again at the forefront in the move to impose cybersecurity requirements directly on industry sectors designated “essential services” or “digital services.” The proposed Network and Information Security (“NIS”) Directive—provisionally agreed by the EU Commission, Parliament and national governments in December 2015 and formally approved in April 2016—requires national governments and designated industry sectors to implement particular programs and protections to “manage risks posed to the security of networks and information systems.”

The Directive covers “essential services industries” that could be severely disrupted by cyberhacking, including energy, transport, banking, financial markets, health, drinking water, and digital infrastructure, which includes internet exchange points and domain registries. It also covers specific “digital services,” namely online
marketplaces, online search engines, and cloud computing services. National governments in the EU must develop an NIS strategy, identify all operators of the essential services in their territories, and ensure that such services:
“take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of networks and information systems which they use.... Having regard to the state of the art, those measures shall ensure a level of security of networks and information systems appropriate to the risk presented....”

Digital services providers are also required to address the security of systems and facilities, incident management, business continuity management, monitoring, auditing and testing, and compliance with international standards. For both essential services and digital services, operators also must notify the relevant authorities of any cyber incidents having a “significant impact” on the continuity of their services. This new Directive mirrors and indeed refers to specific EU rules in the telecommunications and personal data protection areas, which likewise require technical and organizational measures to ensure appropriate security of such data and require the reporting of data breaches.

German Information Technology (“IT”) Security Act. It will be a few years—at least until the NIS Directive is implemented in all EU member countries (currently anticipated by 2018)—until the various details of the NIS Directive requirements are specified and adopted throughout Europe. In the meantime, some European countries have begun similar legislative or industry-collaborative projects. Germany, for example, adopted its own IT Security Act in July 2015, which appoints a responsible authority, calls for an inventory of essential services (including the EU NIS categories, plus food and some additional IT and telecommunications sectors), and requires most of the affected sectors to implement “appropriate organizational and technical measures to prevent failures of the availability, integrity, authenticity and confidentiality of their information technology systems, components and processes, in accordance with the state of the art.” Operators will need to prove their compliance at least every two years, and must report significant breaches to the German Office for Information Security (BSI). There is some scope for industry-agreed standards, but the BSI is charged with approving such standards and reviewing compliance.

Expected secondary legislation will further specify the Act’s coverage. The National People’s Congress of China has also been considering a draft Cybersecurity Law, reflecting the government’s goals to set security standards for technical systems, networks and user data. The law would require government departments in charge of critical information infrastructure to establish security monitoring, reporting systems, early warning, and emergency response plans and drills. In the words of some observers of Chinese legal developments, “the overall thrust ... place[s] the burdens of responsibility on Chinese and multinational companies to protect their users from any potential data breaches.”

China Cybersecurity Law. The National People’s Congress of China has also been considering a draft Cybersecurity Law, reflecting the government’s goals to set security standards for technical systems, networks and user data. The law would require government departments in charge of critical information infrastructure to establish security monitoring, reporting systems, early warning, and emergency response plans and drills. In the words of some observers of Chinese legal developments, “the overall thrust ... place[s] the burdens of responsibility on Chinese and multinational companies to protect their users from any potential data breaches.”

Japan Cybersecurity Basic Act. The Japanese government, working with industry, is also reviewing recommendations for improving protections of Japan’s critical infrastructure and deterrence capabilities as part of its three-year Cybersecurity Strategy adopted in September 2015. Japan’s 2014 Cybersecurity Basic Act already requires infrastructure and cyber-related businesses to take voluntary measures to enhance cybersecurity and cooperate with the government on implementation of relevant measures.

2. CYBERSECURITY REQUIREMENTS FOR GOVERNMENT DEPARTMENTS

Laws requiring government departments to improve management of their own cybersecurity are also appearing around the world—with obvious knock-on effects for these governments’ private-sector contractors and other suppliers, as outlined below.

U.S. In the U.S., the Federal Information Security Management Act of 2002, updated by the Federal Information System Modernization Act in 2014 (collectively “FISMA”), charged the head of every government agency with implementing information security protections that are commensurate with the risk and magnitude of harm to the agency that would result from the unauthorized access, use, disclosure, disruption, modification or destruction of its data or its information systems, or the information systems used or operated by its contractors or others on the agency’s behalf.
Under FISMA, each agency must appoint a Chief Information Officer, and must conduct risk assessments, implement appropriate security measures, implement policies and procedures to manage information security risks, train employees and contractors, periodically evaluate and improve security controls and techniques, and report and manage security incidents. The law puts responsibility on the federal Office of Management and Budget (“OMB”) for overseeing and reviewing agencies’ implementation of information security programs, and for establishing a federal information security incident center (“US-CERT”). OMB has assigned many of its duties to the Department of Homeland Security (“DHS”). The Department of Commerce’s National Institute of Standards and Technology (“NIST”) was made responsible for developing standards, guidelines and other requirements for agencies to use in implementing information security. The General Accounting Office (“GAO”) is responsible for making progress reports to Congress.

The mandate for each federal agency to develop its own information security program, albeit in coordination with OMB, DHS, NIST and GAO, has resulted in programs developing in different ways, for different sectors, at various speeds, motivated by somewhat different policy concerns, and sometimes with certain elements missing altogether. Nevertheless, the U.S. government is intent on making improvements to the information security of all of its agencies, given that “the growing and evolving threats to the systems and networks that support federal operations … can potentially affect all segments of our society, including individuals, private businesses, government agencies, and other entities.”

Internationally. As we have noted, the EU’s NIS Directive places new obligations on European national governments to put their own cybersecurity houses in order. Each national government must adopt a national network and information security strategy, appoint responsible agencies and a single point of contact for NIS issues, develop a risk assessment plan to identify possible risks, and identify measures for preparedness, response and recovery, including cooperation between the public and private sectors. In addition, public sector authorities that qualify as “essential services” will be subject to all of the other requirements of the Directive.

In Australia, where cybersecurity is still largely governed by recommended guidelines and industry frameworks, federal government agencies are required to comply with two particular security frameworks for protecting information and other assets, the Protective Security Policy Framework (“PSPF”) and the associated Information Security Manual (“ISM”). The PSPF and ISM require agencies to use a risk management approach, and to evaluate and take steps to reduce risks in 36 particular areas, including governance (such as management, policies and procedures) and personnel (including training), as well as physical and IT security.

Many other national and state governments are tightening up their cybersecurity programs, not just with respect to technical protections but also through more systematic risk assessment, management and measurement of the broader range of people and process issues that affect information security.

3. CYBERSECURITY REQUIREMENTS FOR PROTECTING TRADE SECRETS

Recent legislative proposals, legislation and cases in the U.S., Europe and elsewhere signal a rush of emerging new mandates about how industry should implement protections—including cybersecurity protections—for valuable confidential business and technical information (“trade secrets”).

The European Union in April 2016 adopted its “Directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure” (“Trade Secrets Directive”). This Directive requires that legally protectable information must have been “subject to reasonable steps
under the circumstances, by the person lawfully in control of the information, to keep it secret.”

This language is mirrored in existing U.S. state law and judicial decisions, and in recent U.S. legislative proposals to expand trade secret protection. The Defend Trade Secrets Act of 2016 (“DTSA”), adopted by the U.S. Congress in April 2016, adds to the current criminal provisions of the Economic Espionage Act (“EEA”) to provide a civil remedy in federal courts against misappropriation of trade secrets. The EEA, similar to the state statutes on which it was based, requires that to qualify as a trade secret, the owner must have “taken reasonable measures to keep such information secret.”

The requirement to employ “reasonable efforts” or to take “reasonable steps” to keep information confidential in order for it to be protected as a trade secret is also included in the WTO Agreement on Trade-Related Aspects of Intellectual Property Rights (“TRIPs”), and required under the laws of developing and developed countries all over the world.

In litigation, courts in the U.S., Russia, Japan and elsewhere have considered a range of cybersecurity procedures as relevant to whether the claimed trade-secret owner has taken “reasonable steps” to keep the information secret. Examples include password protection, restriction of access to those with a “need to know,” use of firewalls, blocking of certain websites, monitoring of employee internet use, implementation of pop-up warnings, prohibition of printing and copying, and restriction of USB-drive usage.

The trend to closely examine a trade-secret owner’s cybersecurity efforts no doubt will continue as the theft of such material by cyberattack proliferates. Cybersecurity therefore has a dual purpose: protecting information against unauthorized disclosure and allowing access to legal process when those protections have failed to prevent misappropriation. “Reasonable steps” by trade-secret owners are required to achieve both goals.

1. SEC CYBERSECURITY RULES AND ENFORCEMENT

The SEC’s general disclosure Regulation S-K has long required public companies to disclose any “material event, trend or uncertainty that is reasonably likely to have a material effect on the registrant’s results of operations, liquidity or financial condition, or would cause reported financial information not to be necessarily indicative of future operating results or financial condition.” SEC Guidance issued in 2011 made clear that certain types of cybersecurity risks and attacks could be sufficiently material to its business or outsourcing to require disclosures under Regulation S-K, including where they involve a material threat to its intellectual property or other assets.

Since 2000, the SEC’s Regulation S-P has also imposed obligations on investment advisers, brokers and dealers to keep non-public customer information confidential and to adopt written policies and procedures to protect such data against anticipated threats and unauthorized access. SEC Guidance has outlined the types of measures it looks for when it examines these companies’ cybersecurity compliance. These include governance and risk assessment, information access rights and controls, data loss prevention and monitoring, vendor management, training, and incident response measures, including the development of an incident response plan.

Litigation in this area to date, particularly litigation brought by the SEC itself, has been described as a “trickle,” but observers “remain convinced that a wave is coming, perhaps a tidal wave, and that it will include not just derivative litigation, but securities class actions and SEC enforcement matters as well.”

The SEC brought and settled an enforcement action against the investment adviser R.T. Jones Capital Equities Management in 2015 for failing to adopt adequate policies and procedures to protect customer data against cyber threats under Regulation S-P. A hack of R.T. Jones’s website—traced back to servers in China—resulted in the theft of

In light of some highly publicized hacks of well-known publicly traded companies, securities laws and shareholder expectations are increasingly demanding that those companies safeguard their confidential information and reputation against cyberattacks—or face administrative penalties and civil damage remedies. This has been particularly true in the U.S., where shareholder litigation and some Securities and Exchange Commission (“SEC”) guidance and enforcement have already been launched. Bills have been introduced in the U.S. Congress to make some of these requirements even more specific.

B. SECURITIES LAWS AND CYBERSECURITY REQUIREMENTS

In light of some highly publicized hacks of well-known publicly traded companies, securities laws and shareholder expectations are increasingly demanding that those companies safeguard their confidential information and
Seven percent of all US residents—16.6 million people—have been subject to identity theft.

— FTC Chairwoman Edith Ramirez
100,000 individuals’ personal data. Among the information security problems noted by the SEC in its settlement order were R.T. Jones’s failure to conduct periodic risk assessments, to use a firewall to protect its web server, to encrypt client data, or to establish procedures for responding to a cybersecurity incident—all of which R.T. Jones promptly fixed. R.T. Jones was fined $75,000 and made subject to a cease-and-desist order against present and future violations.

2. SHAREHOLDER AND RELATED LITIGATION OVER CYBER BREACHES

Shareholder derivative lawsuits in the U.S.—where a class of shareholders sues in the name of the company against its board of directors for allegedly causing harm to the company—have begun to follow cybersecurity breaches, such as the highly publicized incidents at the Target, Wyndham and Home Depot corporations. Related litigation has also been brought against these companies by customers whose data was taken.

a. Target. Four separate derivative lawsuits (and at least nine customer class-action suits) were brought against Target’s directors and officers following Target’s 2013 cyber breach, which allegedly involved 70 million customers’ credit card, PIN and other personal and financial details. A primary claim in these lawsuits was that Target had “less than industry-standard security systems” when compared with the PCI Data Security DSS Standard (“PCI Standard”), an industry standard for large retail institutions that accept credit card and debit card transactions. The complaint alleged that “Target’s deficiencies included the failure to maintain adequate backups and/or redundant systems; failure to encrypt data and establish adequate firewalls to handle a server intrusion contingency; and failure to provide prompt and adequate warnings of security breaches.”

b. Wyndham. A shareholder lawsuit was brought in 2014 against this hotel chain’s directors, following three hacks of Wyndham’s networks in which credit card and other personal information of more than 600,000 customers was taken. The lawsuit claimed that the company failed to implement adequate data security and to timely disclose the breaches, but ultimately was dismissed following proof that the board had diligently attended to the problem and instituted sufficient safeguards for its network.

c. Home Depot. After hackers stole personal and credit card information of approximately 56 million customers, a shareholder derivative suit in September 2015 followed more than 44 other civil suits by consumers and financial institutions, alleging that the company and its directors and officers breached their fiduciary duties of loyalty, good faith and due care, by failing to take reasonable measures to protect this information. Among other claimed failings, the complaint alleged that the company’s IT security systems were “desperately out of date,” and that the defendants were “complacent” in leaving in place “vulnerabilities that not only allowed hackers to enter the system undetected but permitted them to continue siphoning customer cardholder and personal data for almost five months without detection.” The complaint also claimed that the company failed to implement protections specifically required by the payment industry’s PCI Standard.

3. PROPOSED NEW SECURITIES LAWS

Among many bills in the U.S. Congress that could require agencies and industry to manage cybersecurity in more specific ways is the Cybersecurity Disclosure Act of 2015. It would require public companies to disclose in their securities filings whether any members of their board (or other governing body) have expertise or experience in cybersecurity. If not, the company would need to explain how cybersecurity is being taken into account in appointing such persons.

Regardless of whether this or other specific cybersecurity legislation is adopted, there seems to be no doubt that the securities-related cybersecurity obligations of companies, their directors and officers will only continue to grow. In the words of one commentator, “the issue of cybersecurity has emerged at the forefront of risks to be confronted by corporations across a spectrum of industries. Given the catastrophic risks and consequences that have emerged from recent cyberattacks and the litigation, regulatory, and enforcement trends that are driving the evolution of relevant legal standards, both senior executives and directors should be proactive in their oversight and monitoring of the implementation and continued refinement of their company’s cybersecurity controls and processes.”
C. UNFAIR COMPETITION/TRADE LAW REQUIREMENTS RELATED TO CYBERSECURITY

The U.S. Federal Trade Commission, on its own impetus and on the basis of its 1914 legislation prohibiting “unfair or deceptive acts or practices in or affecting commerce,” has stepped up its administrative and court cases against companies that have not implemented sufficient measures against cyberattacks. The FTC asserts that if such companies are misrepresenting the security measures that they are taking to protect consumers’ personal information, and failing to safeguard personal information in ways that damage consumers, they are engaged in unfair and deceptive practices prohibited by the FTC Act.

The highest visibility FTC case to date, a federal district court case against the Wyndham Worldwide Corporation hotel group following the data breaches described above, charged that Wyndham’s security measures were inadequate for failing to include protections such as complex user IDs and passwords, firewalls and network segmentation between the hotels and the corporate network. In addition, the FTC claimed that the company used outdated operating systems that could not be updated with security patches, and allowed improper software configurations resulting in the storage of payment card information in readable rather than encrypted text.

The FTC issued its own guidebook in 2007 entitled “Protecting Personal Information: A Guide for Business,” which the U.S. Court of Appeals cited with approval when it reviewed the case, finding that the FTC had authority over and had given adequate notice of expected appropriate practices related to cybersecurity. (The FTC issued a further, specific “Cybersecurity Guide for Business” in June 2015, which no doubt will also be used as a benchmark in future FTC cases.)

The settlement that Wyndham entered into with the FTC in December 2015 requires the hotel group to implement a “comprehensive information security program” to protect consumers’ cardholder data in compliance with the DSS Standard (or other standard specifically approved by the FTC), and sets out several specific categories of “administrative, technical and physical safeguards” that must be implemented during a 20-year monitoring period. These include:

- Designation of responsible personnel to coordinate and be accountable for the information security program.
- Assessments of material internal and external security risks in each area of relevant operation, including (1) employee training and management, (2) information systems, including network and software design, information processing, storage, transmission and disposal, (3) risks from partner hotels, and (4) prevention, detection and response to attacks, intrusions or other systems failure.
- Implementation of reasonable safeguards to control the identified risks, and regular testing or monitoring of their effectiveness.
- Reasonable steps to select and retain trustworthy third-party service providers, and contractual requirements to implement and retain appropriate safeguards.
- Ongoing evaluation and adjustment of the security program in light of the results of testing and monitoring and other relevant circumstances.

The FTC is seeking even broader scope to bring legal action against companies for failure to protect against cybersecurity breaches. FTC Chairwoman Edith Ramirez testified before the House Energy and Commerce Committee in February 2015 and stated that the Commission supported new laws that would allow the FTC to impose civil penalties as a deterrent against data security violations, give the FTC jurisdiction over non-profit organizations, and require companies to notify consumers of any security breach.

Citing the statistic that 16.6 million persons—or seven percent of all U.S. residents ages 16 and older—had been victims of identity theft in 2012, Ramirez urged Congress: “Never has the need for legislation been greater. With reports of data breaches on the rise, and with a significant number of Americans suffering from identity theft, Congress needs to act.”

II. TIGHTENED GOVERNMENT CONTRACTING REQUIREMENTS
As governments seek to improve their own cybersecurity, they increasingly are insisting that contractors and suppliers that wish to do business with the government closely manage cybersecurity risks at their own firms and with their subcontractors and suppliers.

**U.S.** The U.S. has been the most active in this area to date. The Federal Acquisition Regulations (“FARs”) adopted in the wake of the FISMA legislation described above require all agencies to comply with FISMA in their acquisition planning, and to include appropriate security policies and requirements—including those developed by NIST—in their acquisitions, particularly those involving information technology. Responsibility for how these requirements are implemented so far has been left to individual agencies, with several incorporating some NIST standards expressly into their supplier requirements, such as the Department of Defense (“DoD”), the General Services Administration, and the Department of Health and Human Services.

The DoD has taken the most advanced steps toward requiring government contractors to undertake cybersecurity compliance, under the DoD’s recent “network penetration” rules for protecting various types of “covered defense information” involving “controlled unclassified information.” These will apply mandatory cybersecurity requirements to all relevant defense contract solicitations and impose contract terms to require, among other things, compliance with the protection of information in non-federal information systems and organizations (SP 800-171). It will also require prompt reporting of “cyber events.”

The Department of Health and Human Services (“HHS”) subjects contractors that deal with HHS data or IT systems to a particular security clause that requires compliance with the NIST standards for risk management and security controls in federal information systems, NIST SP 800-37 and SP 800-53. Other agencies have adopted and used a variety of procurement requirements and contract terms governing information security.

The White House issued an Executive Order in February 2013 asking for further comments on and establishing a list of deliverables for the “feasibility, security benefits, and relative merits of incorporating security standards into acquisition planning and contact administration.” The order asked in particular what steps are needed to make these kinds of procurement requirements more harmonized and consistent among government agencies. A joint working group among federal agencies set up under the Executive Order has been assessing ways to improve cybersecurity in federal acquisition and has recommended that the federal government institute baseline cybersecurity requirements as a condition of contract awards for all acquisitions that present cyber risks. The private sector has generally been supportive of making cybersecurity requirements more consistent among the different government agencies’ contract requirements, and the NIST Framework is often mentioned as a basis for developing more consistency among government procurement practices.

**EU.** In addition to imposing new cybersecurity requirements on “critical infrastructure” sectors and EU national governments, the new NIS Directive effectively encourages public authorities to require additional security measures—“beyond what digital service providers would normally offer in compliance with the requirements of this Directive”—when the governments themselves use such services. The Directive contemplates that such additional security measures would be required in the governments’ contracts with such suppliers.

**UK.** Since October 2014, private sector contractors and suppliers to the UK government have had to demonstrate that they comply with the UK’s otherwise voluntary Cyber Essentials Scheme in order to qualify for awards of government contracts that involve the handling of personal information of citizens or government staff, or the supply of IT systems and services that store or process government data classified at least at the “Official” level. Cyber Essentials is a two-tiered system which at the basic level requires five particular technical controls and, at the higher level, integrated information risk management and independent certification.

**Australia.** Companies that provide services to the Australian government must comply with the PSPF and ISM requirements described previously. Australia’s Department of Finance has also developed model cybersecurity clauses that require government suppliers, among other things, to implement protective measures no less rigorous than accepted industry standards, to develop a data protection plan for acceptance by the government department, and to report breaches.
Industries having contracts with the Japanese government are required to abide by security policies based upon its procurement guidelines.99

Governments and the private sector have been busy collaborating in the development of various frameworks and standards designed to help organizations protect confidential information more effectively against cybersecurity breaches. Perhaps the most thorough and broad-based cybersecurity framework to date is the NIST Framework,100 the first version of which was released in February 2014. It takes a risk-based, management-systems approach to assessing and implementing needed protections.

Other formal standards from groups such as the International Organization for Standardization (ISO) are gaining importance, as are general and sector-specific industry frameworks, guidelines and best practices. These have largely started out as consensus arrangements, but compliance with some of these standards is already becoming an express requirement, for example, for companies wishing to participate in certain government contracts. And there are rumblings that the NIST Framework and other similar guidelines may over time become more mandatory, de facto standards against which information security practices are measured, both by regulatory agencies and in litigation.

A. NIST VOLUNTARY FRAMEWORK

The NIST Framework is to date the most comprehensive, risk-based tool for managing information security among different types of businesses and other organizations. Under the 2013 Executive Order described previously, NIST conducted a series of workshops, requests for information and other data gathering among the public and private sectors to develop and share the set of voluntary cybersecurity risk management tools and practices now known as the NIST Framework.

The NIST Framework looks at five principal functions within an organization relevant to cybersecurity—labeled as Identify, Protect, Detect, Respond and Recover—and breaks these into 22 categories and 98 subcategories of activities and outcomes relevant to the development of an effective cybersecurity profile and implementation plan. (An overview of these functions and major categories can be found in Table 1.) The Framework includes a wide spectrum of risk assessment and risk management functions, specific IT and physical security protections, and some broader “people and process” issues such as management oversight, policies and procedures, supplier and other third-party responsibilities, training and communication, monitoring, response planning, and ongoing improvement.

The NIST Framework also cross-references other standards and guidelines, notably NIST SP 800-53, ISO 27001, ISACA’s Control Objectives for Information and Related Technology (COBIT), International Society of Automation’s (ISA’s) security standards, and the Center for Internet Security (CIS) Critical Security Controls. These cross-references clearly indicate that compliance with the NIST Framework can help organizations in their efforts to comply with these other standards and guidelines as well. Indeed, there is some indication that broad acceptance and use of the NIST Framework may become an overall unifying factor in the field of cybersecurity leading practices, which otherwise risks further fragmentation and inconsistency as regulation and standards multiply.

U.S. federal government agencies are enthusiastically embracing the NIST Framework. One recent survey of 150 federal government IT and security professionals found that 82% are using the NIST Framework to improve their security, while 74% say it serves as a foundation for their own cybersecurity roadmap. The annual survey of U.S. government agencies’ cybersecurity practices conducted by DHS and GAO now organizes its detailed questions around the NIST Framework’s five principal functions of Identify, Protect, Detect, Respond, and Recover.101 Several agencies, including the Department of the Treasury, Department of Energy, Federal Communications Commission and...
Department of Justice have also recommended the NIST Framework to industry as best practices for improving cybersecurity in their particular sectors.102

Reviews of the NIST Framework from the private sector and practitioners have also been very positive to date. PwC’s report, enthusiastically entitled Why You Should Adopt the NIST Cybersecurity Framework,103 pointed out that the Framework comprises leading practices from various standards bodies that have proved to be successful when implemented, and that the Framework has potential advantages not only for the “critical infrastructure” sectors at which it was targeted but also for businesses “across virtually all industries.” A recent Tenable Network Security survey of U.S. IT security professionals across a broad range of industries has found that 70% view the NIST Framework as an industry leading practice, with 29% already using this Framework and 14% more planning to do so in the next year.105

Although private-sector companies tend to tailor their cybersecurity programs to their own specific requirements, increasingly these efforts are inspired by or refer expressly to the NIST Framework. Large companies such as Intel, Boeing, Chevron, Walgreens, Pepco, Apple, QVC, Unisys and the Bank of America are using the NIST Framework or planning to do so, and according to NIST, “we also see 50-person firms, like Silver Star Communications in rural Wyoming, describing how the Framework has helped them to be more thoughtful and wiser managers of their cyber risks.”106

The NIST Framework is also being reviewed and considered by governments and the private sector internationally. “Because the Framework could standardize vocabulary and organize cybersecurity requirements across multiple nations, NIST continues to reach out to other governments and major multinational corporations.”107 To address industry concerns that there is a growing diversity of cybersecurity requirements around the globe, NIST itself has been meeting with European and other governments and information security bodies, including the European Commission, the UK, Italy, Poland, Romania, and others, to discuss how the NIST Framework and other approaches could be aligned. In the words of NIST, “some countries and international entities are currently considering adopting an approach that is compatible with the framework established by NIST. Some are even considering adoption of the Framework in its entirety.”108

Under the U.S. President’s mandate and by its express terms, the NIST Framework is voluntary and designed to help organizations manage cybersecurity risks. To date, compliance with the NIST Framework has not been made mandatory as a condition for government contract awards or as a standard against which information security practices have been measured in litigation.

However, the trend to promote such guidelines—and in particular the NIST Framework—seems likely to develop into

<table>
<thead>
<tr>
<th>TABLE 1. OVERVIEW OF NIST FRAMEWORK</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FUNCTION</strong></td>
</tr>
<tr>
<td><strong>IDENTIFY (ID)</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>PROTECT (PR)</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>DETECT (DE)</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>RESPOND (RS)</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>RECOVER (RC)</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
more mandatory requirements to which other cybersecurity measures will be mapped. The NIST Framework is no doubt poised to be the guideline that courts and regulators will use to determine whether companies are managing data security adequately in a whole range of legal contexts. As PwC put it, “In effect, the Framework may become the de facto standard for cybersecurity and privacy regulation and may impact legal definitions and enforcement guidelines for cybersecurity moving forward.”

The NIST Framework is already being cited by NIST and others as a way of complying with other NIST standards that have been made mandatory in some government contracts, such as NIST SP 800-53, which applies to federal information systems, i.e., those operated by the federal government for itself or which a federal contractor operates on behalf of the federal government. The private sector has asked NIST to do further mapping of other such mandatory and voluntary standards requirements to the NIST Framework, and suggested other refinements and improvements.

Just as the FTC’s earlier non-mandatory cybersecurity guidance was used by the U.S. Court of Appeals as evidence that companies had notice of a standard they should be following, there will undoubtedly be similar regulatory, securities and other litigation in the future claiming that companies should have been following the NIST Framework in implementing their cybersecurity program. In the words of one law firm describing what it termed the “growing role” of senior executives and directors in cybersecurity, “As these and other cybersecurity best practices are further developed, implemented, and enforced, corporations that fail to adhere to them may become increasingly vulnerable to enforcement actions and civil litigation.”

However, a major upside to the NIST Framework’s growing popularity and implementation is that it should also help to bring more consistency among what is now a broad diversity of cybersecurity requirements—something industry at large would welcome. Respondents to NIST’s recent consultation requesting feedback on the initial version of the Framework encouraged NIST to continue not only to work with U.S. federal agencies to eliminate duplicative or conflicting regulatory requirements and standards in the cybersecurity area, but also to promote alignment and integration of cybersecurity efforts internationally, consistent with the NIST Framework approach.

### B. ISO 27001 STANDARD

The principal information security standard at the international level at present is ISO 27001, which many companies are implementing and are seeking certification of their compliance. In fact, the NIST Framework—although structured quite differently than this ISO standard—includes and makes numerous references to particular ISO 27001 requirements.

ISO 27001 also takes a risk-based, management-systems approach to information security. It does not establish particular security requirements, but focuses on management-systems controls, including roles and responsibilities; requirements and policies; information management control procedures based on identified risks; training; and monitoring, audits, management reviews and continual improvement.

This standard has proved quite popular among companies internationally, with approximately 24,000 already certificated as compliant as of 2014.

### C. OTHER STANDARDS

Other information and cybersecurity standards are proliferating. As described previously, many government agencies are releasing their own new guidelines and requirements. Sector-specific guidelines and standards are common in the transaction processing, financial services, health care, securities, and other regulated fields. A survey done for the UK government in 2013 identified at least 128 different standards specifically addressing or relevant to cybersecurity, which the report analyzed according to issues of “governance, people, prepare, operations, intelligence and respond.” The number of such standards seems to have increased, rather than decreased, since then.

### IV. IMPLEMENTING LEADING PRACTICES

Cybersecurity tools and standards like the NIST Framework and ISO 27001 are proving useful to companies and other
organizations to assess and implement specific technical controls needed for their IT systems. But just as important, they provide a company with the broader risk assessments and management-systems controls that are needed to develop effective information security programs that go beyond the technical controls. Effective cybersecurity requires the coordinated mix of people, process and technology for organizations to reduce their risks today and on a continuing basis.

In implementing information security systems, all of the relevant technology, people and process issues across the organization must be assessed and managed appropriately. The NIST Framework, consistent with the ISO 27001 standard, goes a long way in defining the broad sweep of issues that a company or other organization needs to consider in developing an effective information security program.

Some commentators have noted that issues beyond the NIST Framework also merit consideration. The NIST Framework does not, for example, fully address the need to assess an organization’s own particular “threat adversaries, their capabilities, and the data they target” when doing a risk assessment and developing appropriate safeguards. It also does not discuss the “statutory, contractual and regulatory obligations” that may apply in implementing cybersecurity. Given that more than 80% of breaches are caused by current and former employees, contractors, service providers, suppliers and business partners, contracts with such parties can be vital for providing specific legal protections and means of redress in case of a breach or loss.

At the time the NIST Framework was released, NIST noted that supply-chain risk management also needed significantly more focus in the future. This vital area has been the subject of a workshop and significant input from businesses in recent months, which will “help inform future versions of the Framework and other cybersecurity and supply chain risk management initiatives.”

The overall risk-management approach of the NIST Framework provides an excellent basis for organizations to implement leading practices as they seek to improve their cybersecurity—not simply to do a “one-time fix” to their IT systems, but to assess and manage the risks to their valuable information intelligently and systematically. The Framework’s “implementation tiers” offer initial guidance on how an organization can measure and improve their information-protection program on a continual basis.

However, initial users of the Framework expressed a clear need for more guidance on how companies can use the results of the Framework to develop a roadmap and get started on practical implementation. This is particularly true for small and mid-sized businesses. Another challenge is how to improve cybersecurity in an organization’s supply chain. With the increasing digitization of supply chains, more and more confidential information is being stored and transmitted between organizations as goods are made, shipped and sold around the world. These trends will dramatically accelerate and increase in the coming decade with the growing use of sensors and the Internet of Things.

In working with global companies on trade secret and information security, The Center for Responsible Enterprise and Trade (CREATe.org) has developed leading practices to help organizations put the appropriate “people and processes” in place to protect valuable know-how. CREATe believes that organizations need to strategically allocate resources to best protect trade secrets and confidential information. To do this, an organization must understand what is most important to protect and what specific risks are most likely to occur. The focus on prioritizing what to protect complements the NIST Framework which focuses on how to protect information and recover from breaches. The CREATe approach measures the maturity of current business processes, gains expert insights and identifies target areas for improvement. CREATe’s work is consistent with and can be mapped to the NIST Framework and ISO 27001 methodology. Leading trade secrets lawyer James Pooley has described the CREATe.org Leading Practices service as an “excellent resource” for information security check-ups.

Using the NIST Framework and taking such a systematic risk-assessment and management-system approach to its implementation can not only help to integrate cybersecurity into an organization’s overall risk management and compliance program, but also help to ensure that all of the technology, people and process issues across the organization that are relevant to cybersecurity are assessed and managed effectively.
Cybersecurity breaches continue to be front-page news. Statutory, regulatory and court-mandated requirements to manage information security effectively are becoming more and more pervasive. Now more than ever, companies and governments need to work together—and are doing so in the NIST Framework—to develop and utilize a common approach to information security that addresses people, process and technology. The NIST Framework provides a useful tool for companies seeking to do business with the government, to satisfy securities, privacy and trade secrets laws, to meet contractual confidentiality undertakings, and generally to protect the value of commercial secrets. Given the regulatory tsunami, the use of the Framework may become virtually, or actually, mandatory for companies selling to the U.S. government or critical infrastructure industries. The weak link in any cyber security program is the end-user. This creates more and more challenges as employees work remotely, organizations use more contractors and virtual teams and supply chains become more complex with more parties involved.

The overall goal of a program is not just to manage the vital area of cybersecurity effectively within companies and other organizations. It is also to do so efficiently and cost-effectively, avoiding the fragmentation and duplication of effort that has cost billions of dollars in other compliance areas, like labor, where there are more than 10,000 corporate and industry standards/codes, and where any one company can face more than 30 labor compliance audits in one year—all mapping to slightly different requirements.

The challenge for each company and organization is to embed data security effectively into how the organization operates overall. As pointed out previously, 80% of cyber breaches are linked to current and former employees, contractors, service providers, suppliers and business partners. Companies considered leaders in this area have consistently told CREATe.org that the weakest link in their program is the end-user—whether an inside employee or third-party organization. It is clear that engaging insiders about information security will require a cross-functional effort. Human resources, risk management, legal, sourcing, marketing and operations will all need to work with their IT department to create practical procedures that strengthen security while supporting the business realities and needs of each functional area in the company. Large enterprises will need to understand how programs can be scaled in a practical way to the small and medium companies that are part of their value chain. Ultimately, information security needs to be viewed as a journey of continual improvement involving people, process and technology.

In the rising tide of cybersecurity regulation, implementing effective cybersecurity programs will require a comprehensive approach that goes beyond mere technical fixes. A careful assessment of the likely risks to an organization’s confidential information, and a specific, ongoing plan to address each of the significant risks among the organization’s relevant technology, people and process areas, internally and with its relevant supply chain, are becoming increasingly important—both operationally and legally—in protecting valuable information against theft and misuse.
REFERENCES


4 Gramm-Leach Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (Nov. 12, 1999), https://www.gpo.gov/fdsys/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf. Under Section 501(b), GLBA requires relevant agencies to “establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards—(1) to insure the security and confidentiality of customer records and information; (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.”


6 Id. at § 314.3; see generally FTC, Safeguarding Customers’ Personal Information: A Requirement for Financial Institutions (May 2002), https://www.ftc.gov/tips-advice/business-center/guidance/safeguarding-customers-personal-information-requirement.

7 16 C.F.R. § 314.4.

8 Id.


12 45 C.F.R. § 164.306(a).


18 Id., Annex II.

19 Id., Annex III.

20 Id., arts. 14(1a), 15a(1).

21 Id., art. 15a(1).

22 Id., arts. 14(2), 15a(2).

REFERENCES, CONT.


25 Id., secs. 8a-8c.


34 44 U.S.C. § 3544(a)-(c).


39 NIS Directive, supra note 17, arts. 5-6.

40 Id., Recital linked to art. 14.


46 Id., art. 2(1)(c).


For example, “In Russia, the possessor of such information must implement a “regime” of trade secrecy, which must include defining a list of information constituting commercial secrets, limiting access to that information by establishing a procedure for handling the information and for control over compliance with that procedure, keeping a record of persons who acquired access and/or to whom that information was furnished or transferred, regulating use by employees on the basis of labor and civil law contracts, and affixing a “commercial secret” stamp specifying the holder of that information.” Id. at 5, citing Russia - Federal Law of the Russian Federation on Commercial Secrecy, No. 98-FZ 2004, art. 3(2), http://www.wipo.int/edocs/lexdocs/laws/en/ru/ru048en.pdf.


A SEC examination and report on more than 100 such firms in 2015 provided an interesting insight into the risk-based approach to cybersecurity that the SEC is expecting. See SEC, Off. of Compliance Inspections & Examinations, Risk Alert: Cybersecurity Examination Sweep Summary (Feb. 3, 2015), https://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf.

63 Collier v. Steinhafel, supra note 62, para. 74.


52 See id. at 5, 7, 9-11, 17. For example, “In Russia, the possessor of such information must implement a “regime” of trade secrecy, which must include defining a list of information constituting commercial secrets, limiting access to that information by establishing a procedure for handling the information and for control over compliance with that procedure, keeping a record of persons who acquired access and/or to whom that information was furnished or transferred, regulating use by employees on the basis of labor and civil law contracts, and affixing a “commercial secret” stamp specifying the holder of that information.” Id. at 5, citing Russia - Federal Law of the Russian Federation on Commercial Secrecy, No. 98-FZ 2004, art. 3(2), http://www.wipo.int/edocs/lexdocs/laws/en/ru/ru048en.pdf.


57 A SEC examination and report on more than 100 such firms in 2015 provided an interesting insight into the risk-based approach to cybersecurity that the SEC is expecting. See SEC, Off. of Compliance Inspections & Examinations, Risk Alert: Cybersecurity Examination Sweep Summary (Feb. 3, 2015), https://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf.


1. Install and maintain a firewall configuration to protect cardholder data;
2. Do not use vendor-supplied defaults for system passwords and other security parameters;
3. Protect stored cardholder data;
4. Encrypt transmission of cardholder data across public networks;
5. Use and regularly update anti-virus software or programs;
6. Develop and maintain secure systems and applications;
7. Restrict access to cardholder data by business need to know;
8. Assign a unique ID to each person with computer access;
9. Restrict physical access to cardholder data;
10. Track and monitor all access to network resources and cardholder data;
11. Regularly test security systems and processes; and
12. Maintain a policy that addresses information security for all personnel.

63 Collier v. Steinhafel, supra note 62, para. 74.


REFERENCES, CONT.

Role%20of%20Senior%20Executives%20and%20Directors.pdf.
72 Id., para. 24.
76 Id., at 4-6.
78 Id.
79 FAR § 7.103(w), https://www.acquisition.gov/far/html/Subpart%207_1.html.
85 Some questions have arisen as to exactly how these new rules will work and when exactly compliance by government contractors will be required, issues as to which the private sector has been providing input to the DoD. See R. Metzger, Twists and Turns—DoD Backs Away from the ‘Network Penetration’ DFARS or Does It?, 105 Fed. Contracts Rep. (Feb. 16, 2016), http://www.rjo.com/PDF/bloomberg_BNA_02162016_RSM.pdf.
86 See Bodenheimer, supra note 83, at 17.
89 See Bodenheimer, supra note 83.
91 Section 8 of the Executive Order, id., established a “Voluntary Critical Infrastructure Cybersecurity Program,”” to be coordinated among multiple federal agencies. Section 8(e) directs an inter-agency effort to assess the “feasibility, security benefits, and relative merits of incorporating security standards into acquisition...
planning and contract administration.” Under Section 8(e), GSA and DOD established a Joint Working Group on Improving Cybersecurity and Resilience through Acquisition.  


95 NIS Directive, supra note 17, recitals 53, 55.


97 See Srinivas, supra note 41, at 17.


104 Id. at 1.


107 Id. at 2.

108 Id.

109 PwC, supra note 104, at 5.

110 The NIST Framework itself cross-references its subcategories to NIST SP 800-53 ninety-six times. NIST SP 800-171 lists in a table its requirements for protecting controlled unclassified information and maps these directly to similar requirements in SP 800-53 and ISO’s 27001 standards, with a reference to the fact that such controls can be found in the Cybersecurity Framework’s categories and subcategories. It notes that this information can be useful to organizations “that wish to demonstrate compliance … in the context of their established information security programs, when such programs have been built around the NIST or ISO/ IEC security controls”. NIST, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations, at ix. (2015), http://csrc.nist.gov/publications/drafts/800-171/sp800_171_second_draft.pdf.

111 Comments of Ernst & Young on Cybersecurity Framework RFI (Feb. 22, 2016), at 6 (“NIST should develop, maintain, and publish a mapping that provides a holistic view of all U.S. cybersecurity regulatory requirements and mandated standards across industry sectors. This will prevent duplication between requirements and standards”), http://csrc.nist.gov/cyberframework/rfi_comments_02_2016/20160222_Ernst_&_Young.pdf. See generally NIST, Analysis of Cybersecurity Framework RFI Responses (Mar. 24, 2016), http://www.nist.gov/cyberframework/upload/RFI3_Response_Analysis_final.pdf.

112 Comments of Ernst & Young on Cybersecurity Framework RFI (Feb. 22, 2016), at 6 (“NIST should develop, maintain, and publish a mapping that provides a holistic view of all U.S. cybersecurity regulatory requirements and mandated standards across industry sectors. This will prevent duplication between requirements and standards”), http://csrc.nist.gov/cyberframework/rfi_comments_02_2016/20160222_Ernst_&_Young.pdf.

113 NIST, Analysis of Cybersecurity Framework RFI Responses, supra note 112, at 15, 17.

REFERENCES, CONT.


116 PwC, supra note 104, at 6.

117 PwC, supra note 1.


ABOUT THE CENTER FOR RESPONSIBLE ENTERPRISE AND TRADE (CREATE.ORG)

The Center for Responsible Enterprise And Trade (CREATE.org) is a non-governmental organization (NGO) helping companies around the globe prevent piracy, counterfeiting, trade secret theft, and corruption.

Our mission is to make leading practices in IP and trade secret protection and anti-corruption achievable for all companies. CREATE works across diverse industries in countries around the world to provide cost-effective and practical assessments, independent evaluations, training and other resources for safeguarding IP and trade secrets and preventing corruption.

To achieve this mission, we have developed CREATE Leading Practices for IP Protection, CREATE Leading Practices for Trade Secret Protection and CREATE Leading Practices for Anti-Corruption, services based on best practices drawn from multinational companies, academics, international and business organizations.

Building on decades of work across the business community on quality assurance, health and safety and other issues, CREATE takes a management systems approach to helping companies implement the internal business processes they need to effectively protect intellectual property and prevent corruption.

Companies around the world are using CREATE Leading Practices to benchmark and improve systems for IP protection and anti-corruption. The services are available in a variety of languages including Chinese, Japanese, English, Portuguese and Spanish.

FOR MORE INFORMATION

Please visit www.CREATE.org, via email at info@create.org or follow us on Twitter @CREATE_org.

©2016 CREATE.org All Rights Reserved.