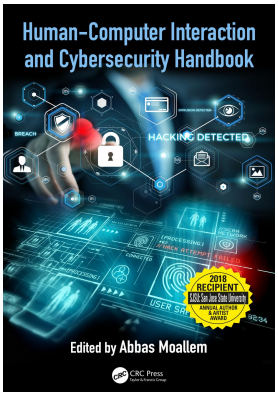

Human-Computer Interaction and Cybersecurity Handbook

Abbas Moallem

US cybersecurity and privacy regulations

Publication details
https://test.routledgehandbooks.com/doi/10.1201/b22142-14
Mark Schertler, Jill Bronfman
Published online on: 24 Oct 2018

chapter fourteen

US cybersecurity and privacy regulations

Mark Schertler and Jill Bronfman

Contents

14.1 Cybersecurity law compliance basics

14.1.1 *Episodes of* Homeland

People have made a joke about the television show *The Walking Dead*: every episode has the same plot. We need supplies! The supplies are over there! But there are zombies over there! The problem inherent in this dilemma is obvious, and there will be casualties.

This same scenario plays out in nearly every episode of *Homeland*, a television series available on the Showtime network that dramatizes US data security and privacy issues. The name of the show itself is a reference to the actual Department of Homeland Security (DHS), a federal government agency tasked with protecting the US from terrorism and other threats to the security of the nation (US DHS, 2017).

On *Homeland*, Carrie is the central character in a series of dramatic episodes involving national security, including physical security and data security. On any given episode, Carrie needs some data, aka electronic documents. They are in a secure facility/server/behind a firewall with a password. But if she goes and gets them, she will get killed! Why? Everything the average person does is tracked online.

- Financial data: If Carrie uses a credit card to travel, that information is stored as data on a server. If anyone tracks where she spends money, she will be found.
- Healthcare information: If someone gets shot, they cannot go to a regular hospital, because in order to get medical care, you need to give out an extraordinary amount of personal and health data, and you can be found.
- Telecommunications and communications transmissions: Even pre-Internet, or really pre-web, most of the developed world was connected via the landline telephone network. Location data has always been available for landline calls, which enables the 911 network. E911 identifies your location on your cell.

Yet, it is a television show, and poor beleaguered Carrie has a limited amount of time to save the day. So what Carrie would often do is persuade someone to let her in (password), wear a disguise (use someone else's account), or carry a gun (hack/brute force). Nevertheless, they always find her and sometimes she gets several significant scratches on her nose.

14.1.2 *Introduction to cybersecurity*

Why do we need to know about cybersecurity in order to save the day? What are the risks we are trying to minimize? A myriad of new jobs are available in the cybersecurity field, mostly created in an attempt to answer these two questions. There are newly focused cybersecurity-specific professions, including audit, compliance, and risk management. In addition, there are entirely new job categories for privacy professionals, security experts, and privacy-trained product counsel. Let us say you are assigned one of these roles in your new job. What can you learn in order to shine in your new position and/or profession?

There are big picture issues that you can apply to various scenarios. Corporate compliance may demand competing requirements. When you are directly dealing with a business unit, what is the goal? Look to the legal and information technology (IT) departments to create direction and training for entry-level employees. Creating a corporate compliance structure for privacy and security is a more elaborate exercise and requires a different skill set than would have previously been sufficient for advising a chief executive officer.

The risks associated with data security and privacy law failures are myriad. The most obvious and familiar is data breach, and its associated financial and legal liabilities, including state government-required reporting. The Federal Trade Commission (FTC) keeps tabs on companies who act in unfair and deceptive ways toward the public, including breaches and substandard security practices. The payment card industry (PCI) imposes additional standards for the use of credit card data. Business to business (B2B) and business to consumer (B2C) contracts may impose obligations on companies to maintain certain cybersecurity minimums standards and/or leave an open obligation to comply with industry standards, generally or with regard to specific named standards. The liability for negligence outside of contracts, and in addition to them, concerns many companies who fear a moving target standard of care for how much security will be expected and whether hindsight is required after an unforeseen, but perhaps not unforeseeable, breach. Shareholder derivative lawsuits loom in the shadows, with some of the same concerns mentioned for general liability about rapidly updating technology applied in the cybersecurity field and whether a company, especially a small company with limited resources, will be expected to keep up.

14.1.3 Players and playbooks: Who controls corporate privacy and data security

14.1.3.1 Legal standards

Cybersecurity law in the United States is a patchwork quilt of regulations, including some antiquated regulations that govern a small sector of federal government agencies, such as the Privacy Act of 1974 (US Department of Justice, 2017). This so-called Privacy Act followed a Watergate-era concern with government intrusion into the personal lives of average citizens. In actuality, the scope of this Privacy Act could not imagine the extent to which the National Security Administration and other federal and state government agencies would have access to citizens' data. This expansion in scope and breadth to the collection of data is enabled by, first, the expansion of hardware and software technologies that can interact with humans and, second, by the types of data we voluntarily, and sometimes involuntarily, share with other individuals, corporations, and the government.

14.1.3.2 Corporate culture

Corporations vary in their cultural responses to the primacy of data collection, processing, and storage in the twenty-first century. In nearly all cases, corporations are collecting data, although they often outsource the processing and storage of data. Increasingly, this processing of data is done by subcontracted specialists, and the storage of data is often off site, remote, and possibly beyond the reaches of the US Government to access the data by subpoena or other legal process.

Corporations are attempting to keep pace with rapid changes in technology, and the ability of the legal profession to reflect changes in technology is often limited to revising B2B contracts that are only reviewed and revised every 1–3 years. Further, products and services are designed, implemented, and thrust upon the market periodically, but without full understanding of the consequences of their ability to collect and store personal data.

14.1.3.3 Process improvements

Most companies begin their cybersecurity assessments with an audit of data location and an evaluation of existing processes. Obvious process improvements center upon a more consistent review and audit of data collection procedures and processes. Once a year as a standard protocol may no longer be enough for a privacy impact assessment (PIA) or data mapping exercise. Education and training supporting these procedures are crucial.

Less obvious, and perhaps more onerous, suggestions include reformulating how we do business around data collection. Should legal and policy procedures for the collection of personal data continue to be largely left to the private sector? Or should the inroads made by the sectoral regulation of certain industries, described in the next section, be made universal, in order to protect data privacy across industries and across the United States?

Further, ideally, the audit or assessment is not the first time a company has considered how its actions affect its customers, employees, and vendors. Privacy by design is a movement to imbed privacy considerations into products and services at the onset, rather than as an add-on layer after the design is completed or even after lawsuits or government prosecution yields a consent decree mandating privacy and security be added.

14.1.4 Sectoral regulation overview: Case law, statutes, and agency regulation

14.1.4.1 Financial regulations: Gramm–Leach–Bliley

The Gramm–Leach–Bliley Act (GLBA) (US FTC, 2002) was enacted to require financial institutions, according to the FTC, to disclose their data security and privacy practices to their customers and to create security protocols for their customer's personal data. Financial institutions are defined broadly by the GLBA, including not only banks that hold personal funds, but also institutions that loan money or offer insurance. The regulation covers those who render financial advice as well, in keeping with the understanding of the responsibility for private financial data at the time in which the legislation was drafted. This law created not only an industry of tools to comply with the law, but also an army of personnel associated with compliance. Further, this law, along with healthcare privacy and security regulations described below, kicked off a movement in the legal, compliance, and IT fields toward outward-facing compliance and information sharing among companies rather than just establishing privacy and security standards on a case-by-case, company-by-company basis.

14.1.4.2 Healthcare: Health Insurance Portability and Accountability Act

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 began with an acknowledgement that medical records were increasingly becoming electronic and needed to be accessible by medical professionals. Arguably, the security and privacy requirements, while a "side effect" of this medicine, may have had the most lasting impact on the public. Covered entities, the healthcare providers, must adhere to security and privacy protective requirements for the public. The goal is to protect personal health information (PHI) now unleashed from the locked file cabinet in the doctor's office onto the world of electronic storage.

The act covered both privacy and security issues and defined for many the distinction between the two. The security requirement reads as follows: "The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality,

integrity, and security of electronic protected health information" (US Department of Health and Human Services, 2017a). Security was focused on the safety of the data, whereas privacy rules protected individuals. The privacy rule adds that "the HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, healthcare clearinghouses, and those healthcare providers that conduct certain healthcare transactions electronically. The Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization" (US Department of Health and Human Services, 2017b).

The HIPAA-covered entities will contract with companies who carry this information forward, by storing it or processing it, and these companies, called business associates under the law, have similar obligations to protect the covered entities' patients. In addition, the breach notification rule also requires HIPAA-covered entities and their business associates to notify those affected by a breach of their protected health information.

14.1.4.3 Telecom: Federal Communications Commission regulation

The Federal Communications Commission (FCC) ventured into the field of data privacy regulation with its Customer Proprietary Network Information (CPNI) (US FTC, 2002) restrictions. CPNI regulation was intended to limit the ability of telecommunications provider to take customer information gathered to provide one service and use it to market another service to that customer (US Government Printing Office, 2011). These laws became more and more relevant as companies began mergers, acquisitions, and joint ventures in a deregulated marketplace in the late 1990s and into the first decade of the twenty-first century. CPNI regulations attempt to create a bridge between the commercial efficiencies of using personal information gathered about existing customers and the privacy interests of customers. Several exceptions have evolved to this general principle in the law, including exceptions for emergencies and consent of the customer. In an acknowledgement of the specially situated regulated position of telecommunications providers, providers are allowed to use depersonalized, aggregated information, but only if the providers also allow others to use the same aggregated information, for a reasonable fee. Into the following decade, the technological ability to collect and share personal data has grown into a substantial industry, and it will be interesting to see how regulated versus unregulated companies deal with personal data over the next few years.

14.1.4.4 Utility and technology rulings: Federal Trade Commission regulation

The Federal Trade Commission (FTC) has gone head to head with the FCC over primary federal agency jurisdiction over security and privacy issues. The FTC relies on Section 5 of the FTC Act for its authority over these issue, but it is limited by the scope of the FCC's authority over some carriers. Section 5 of the FTC Act is general rather than specifically related to either security or privacy in that it prohibits unfair or deceptive practices by companies in their business practices. On its website, the FTC lists a broad variety of privacy-related acts to which it may enforce, including the Truth in Lending Act, the CAN-SPAM Act (for e-mail practices), the Children's Online Privacy Protection Act (protecting the personal information of children under 13), the Equal Credit Opportunity Act, the Fair Credit Reporting Act, the Fair Debt Collection Practices Act, and the Telemarketing and Consumer Fraud and Abuse Prevention Act (US FTC, 2015). As a result, the FTC has had several enforcement actions against companies to call out violations of these acts, and to, under its more general Section 5 authority, notify companies of insufficient privacy and data security practices.

14.1.4.5 Federal: FISMA and Federal Risk and Authorization Management Program

Recognizing the need to address cybersecurity incidents that affect the US Government, the US Congress has passed two different acts both with the acronym "FISMA" to improve the information security posture of systems used by the US Government for information processing. The first is the Federal Information Security Management Act of 2002 (FISMA 2002), which "requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other sources" (US NIST, 2017).

The follow-up is the Federal Information Security Modernization Act of 2014 (FISMA 2014), addressing the lessons learned and increased technological complexity and risk that surfaced in the intervening 12 years, "amends the Federal Information Security Management Act of 2002 (FISMA) provides several modifications that modernize federal security practices to address evolving security concerns. These changes result in less overall reporting, strengthens the use of continuous monitoring in systems, increased focus on the agencies for compliance, and reporting that is more focused on the issues caused by security incidents" (US NIST, 2017). The evolving FISMA acts promotes a risk-based approach to the implementation of cybersecurity policies and controls at an agency level so that each individual agency can address the risks to its mission in an appropriate manner versus a one–size-fits all solution for the entire US Government. There is centralized control that is mandated including the development of security standards, guidelines and minimal requirements by the US National Institute of Standards and Technology (NIST), development of appropriate government-wide information security policies by the Office of Management and Budget, and development of government-wide security incident reporting and agency annual reporting requirements by the DHS.

Federal Risk and Authorization Management Program (FedRAMP) is a US federal government-wide program for the assessment and authorization of cloud services providers. It follows FISMA guidelines and uses NIST 800-53 controls to define its cybersecurity requirements. FedRAMP applies to software-as-a-service, platform–as-a-service, and infrastructure-as-a-service providers. It provides a "do once, use many time" framework (US FedRAMP, 2017) for both cloud service providers and US agency buyers. Cloud service providers can be accessed against FedRAMP requirements and achieve an authority to operate (ATO). All US agency buyers when looking for cloud services can then review the ATO and know that the service provider has been assessed and meets the required cybersecurity controls to protect US Government data.

14.1.5 State regulation overview

14.1.5.1 State data breach/privacy regulations

Due to the failure to pass comprehensive US federal cybersecurity and privacy regulations, states have stepped in and started passing regulations governing aspects of cybersecurity themselves. As of this writing, 48 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have passed personal identifiable information (PII) breach disclosure laws. These state laws differ, in some cases significantly, as to what qualifies as PII. The definition of PII of most states is a combination of basic identification information such as name, social security number, state identification (ID) (driver license information), and financial account data. Various states include additional information in their PII

definition including biometric information, DNA (as of this writing, only Wisconsin codifies this in law), electronic signature (as of this writing only, North Dakota codifies this in law), medical information, date of birth, employee ID, mother's maiden name, health insurance information, and tax information. In addition to differences in what constitutes PII, what constitutes a breach, who must be notified, and when and what type of disclosure is required also differ from state to state. Further, some states specify the content of the breach notification. These state breach laws are constantly being amended, and new related regulations are becoming law. The National Conference of State Legislatures (2017) has resources for tracking the constantly changing landscape of state cybersecurity and breach notification legislation.

While it is a positive step forward for citizens of states that have breach notification regulations, it is a burden on organizations that do business across state lines as differing requirements of each state can overlap or contradict each other creating a complex breach notification environment. It would seem that a unified federal breach notification law would be advantageous, but several states are worried that a federal regulation would offer their citizens less protections than their current state laws (National Law Review, 2017). It is difficult to pass federal legislation that would preempt all state regulations due to political constraints, and therefore, any federal legislation would simply add another overlapping set of standards.

14.1.5.2 New York state cybersecurity requirements for financial services companies

Another example of states stepping in due to the lack of US federal cybersecurity regulations is the New York state cybersecurity requirements for financial services companies, which went into effect on March 1, 2017. The law was passed by the New York state legislature to address increasing threats posed by cyberattacks on institutions, particularly financial institutions, and is the first state regulation to address these cybersecurity threats. "This regulation requires each company to assess its specific risk profile and design a program that addresses its risks in a robust fashion" (New York State Department of Financial Services, 2017). The law applies to any person or nongovernment entity, defined as a covered entity, operating under the banking, insurance, or financial services law in the state of New York.

The law requires each covered entity to develop and maintain a cybersecurity program based on a risk assessment of its internal and external cybersecurity risks. Specific components of a cybersecurity program that are required include the following:

1. Cybersecurity policy—The regulation specifies and outlines a policy or policies that must be written, maintained, and approved by a senior officer, the board of directors, or an appropriate governing body.
2. Chief Information Security Officer (CISO)—A CISO must be designated, and that person is responsible for the development, implementation, and enforcement of the cybersecurity program.
3. Penetration testing and vulnerability assessments—The regulation requires monitoring and testing to evaluate the effectiveness of the cybersecurity program. It states that monitoring should be continuous, or penetration testing is required at least annually and vulnerability assessments are required at least biannually.
4. Audit trails—Cybersecurity audit trails that allow detection and response to cybersecurity events must be implemented and records maintained for at least 3 years.

5. Access privileges—Covered entities shall limit access privileges and regularly review existing privileges.
6. Application security—A cybersecurity program must put in place policies, guidelines, and procedures for all internally developed application software to ensure that secure development practices are followed, assessments are performed, and testing on all externally developed application software is performed to determine the risk third party software may introduce.
7. Risk assessment—The risk assessment previously mentioned must be conducted periodically, and the cybersecurity program must be able to adapt to the new and evolving risk identified in the assessment.
8. Cybersecurity personnel and intelligence—The covered entity must utilize qualified personnel and must ensure that these personnel receive adequate training, including training on the changing cybersecurity threat landscape.
9. Third-party service provider security policy—Similar to the internal security policies, a covered entity must also implement, maintain, and enforce security policies that apply to third-party service providers that have access to covered entities' systems or nonpublic information.
10. Multifactor authentication—Covered entities must implement multifactor authentication or similar controls for access to systems and nonpublic data. In particular, access to internal networks from external networks is called out.
11. Data retention—The regulation requires policies addressing the retention and secure disposal of nonpublic data.
12. Training and monitoring—In addition to the training required for cybersecurity personnel, all authorized users must be monitored and trained as well.
13. Encryption of nonpublic information—Encryption of nonpublic information over external networks and at rest on covered entity systems is required. If encryption is not feasible, compensating controls must be implemented, and these controls must be annually reviewed by the CISO to determine if they are still effective and if encryption has become feasible since the last review.
14. Incident response plan—The covered entity shall have a written incident response plan to address cybersecurity events.

In addition, the law requires covered entities to notify the superintendent of the New York State Department of Financial Service if a cybersecurity event occurs that must be reported to other government agencies under other laws or may materially harm any part of the covered entity's operations. Covered entities must also annually provide written certification that it is in compliance with this regulation. To encourage the required information sharing, the regulation does exempt covered entities from the disclosure of information under other New York state and federal laws.

The New York state cybersecurity requirements for financial services companies is the first cybersecurity regulation of its type in the United States, and being just months old at the time of this writing, it will be interesting to see the effect it has on cybersecurity regulations at the state and federal levels in the United States. In general, companies who operate nationally often set their company policies according to the strictest security standards in place in states in which they operate. As a result, one state can set industry standards on a national level, and a small number of companies who operate nationally can model industry standards for many regional and smaller companies.

14.2 Industry standards and the role of corporations

14.2.1 Creation of industry standards

Again, due to the lack of US federal cybersecurity regulations and a myriad of state actions, industry players have developed and advanced standards for security and privacy. A couple of the best known are the Payment Card Industry Data Security Standard (PCI DSS) and the Health Information Trust Alliance (HITRUST) common security framework (CSF). In addition, the NIST cybersecurity framework, while developed by the US Government as a nonbinding framework for critical infrastructure, is slowly being adopted by many different industries as a standard framework to follow to assure that adequate risk-based cybersecurity programs are implemented. Industry standards function to provide consistency for companies to plan their budgets, hire personnel, and shield themselves from liability and government scrutiny.

14.2.1.1 PCI DSS

The PCI Security Standards Council is a global organization founded by some of the largest payment card processing companies—American Express, Discover Financial Services, JCB International, MasterCard, and Visa Inc.—in the world. The Security Standards Council develops and promotes payment card industry standards for the protection of cardholder data. All five founding members have agreed to abide by the standards developed and require their vendors and processors to do so as well. To validate that their standards are being properly followed, the council also has a program to train, test, and accredit assessors to validate that those who process and/or store payment card information are properly following the council's standards.

The most well-known standard developed by the council is the PCI DSS. PCI DSS is an evolving standard and is currently at version 3.2. The PCI DSS defines technical and operational requirements for the protection of payment card account data. "PCI DSS applies to all entities involved in payment card processing including merchants, processors, acquirers, issuers, and service providers. PCI DSS also applies to all other entities that store, process or transmit cardholder data (CHD) and/or sensitive authentication data (SAD)" (PCI Security Standards Council, 2016). Cardholder data consists of primary account number, cardholder name, expiration data, and service code. Sensitive authentication data includes the full track data on the magnetic stripe or chip equivalent, card validation value, and PIN data. PCI DSS covers the following six high-level areas:

1. Build and maintain a secure network and systems
2. Protect cardholder data
3. Maintain a vulnerability management program
4. Implement strong access control measures
5. Regularly monitor and test networks
6. Maintain an information security policy

14.2.1.2 HITRUST CSF

The HIPAA regulations, as outlined earlier, and, specifically for our discussion in this section, the security and privacy rules were written to apply to a wide range of healthcare organizations, for example, everything from a small doctor's office to a large healthcare organization. As a regulation should be, it identifies requirements for protecting electronic

PHI (ePHI), but makes no recommendations on what controls to use or how to meet those requirements. This led to the requirements being generic, making it is very subjective as to what is required to be HIPAA compliant. The HITRUST is a healthcare industry-focused nonprofit that has developed a CSF for protection protecting healthcare information and ePHI. The HITRUST CSF was developed to provide a risk-based and compliance-based approach and provide a prescriptive framework of controls.

The HITRUST CSF:

- Includes, harmonizes and cross-references existing, globally recognized standards, regulations and business requirements, including ISO, NIST, PCI, HIPAA, and State laws
- Scales controls according to type, size, and complexity of an organization
- Provides prescriptive requirements to ensure clarity
- Follows a risk-based approach offering multiple levels of implementation requirements determined by risks and thresholds
- Allows for the adoption of alternate controls when necessary
- Evolves according to user input and changing conditions in the industry and regulatory environment on an annual basis
- Provides an industry-wide approach for managing Business Associate compliance" (HITRUST Alliance)

14.2.1.3 NIST cybersecurity framework

While the US Government has no general-purpose cybersecurity or privacy regulations at present, it has directed the creation of a cybersecurity framework. On February 12, 2013, then President Obama signed an executive order (EO), which, among other things, including improving cybersecurity information sharing with the US private sector, directed the US NIST to create a "Baseline Framework to Reduce Cyber Risk to Critical Infrastructure." The EO directed NIST to create a cybersecurity framework that would "enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties" (White House, 2013). The cybersecurity framework, officially titled the "Framework for Improving Critical Infrastructure Cybersecurity" was completed and officially released by NIST 1 year later on February 12, 2014.

The cybersecurity framework promotes a risk-based approach to cybersecurity. It defines five parallel and continuous cybersecurity functions—identify, protect, detect, respond and recover—that should be evaluated to "help identify and prioritize actions for reducing cybersecurity risk" (US NIST, 2014). For each function, the cybersecurity framework defines categories and subcategories of activities and outcomes pertinent to the function to help evaluate needs and risks. Informative references for each function identify already developed NIST and industry standards, guidelines, and best practices that provide further detail for the function. These functions and related information are called the Framework Core.

Next, the cybersecurity framework defines tiers to help an organization understand their level of sophistication related to the implementation of cybersecurity and risk management. Tiers are based on an "organization's current risk management practices, threat environment, legal and regulatory requirements, information sharing practices, business/mission objectives, cyber supply chain risk management needs, and organizational

constraints" (US NIST, 2014). The tiers defined in the cybersecurity framework are the following:

- Practical (tier 1)
- Risk Informed (tier 2)
- Repeatable (tier 3)
- Adaptive (tier 4)

The cybersecurity framework points out that not every organization needs to be at tier 4 but should rather strive to obtain the tier that reduces their cybersecurity risk and is most cost-effective to obtain.

Finally, the cybersecurity framework defines a profile for aligning the Framework Core functions, categories, and subcategories with the business requirements, risk tolerance, and resources of the organization. The cybersecurity framework recommends developing a current profile describing the current state of cybersecurity activities within the organization and a target profile for defining the desired state the organization would like to work toward. The gaps between the current and target profiles will identify the action items that organization needs to take on to improve its risk management and cybersecurity posture.

The cybersecurity framework is intended to be a living document changing with the cybertechnology and risk landscape. To ensure this, on December 18, 2014, the US Congress passed the Cybersecurity Enhancement Act of 2014, "to provide for an ongoing, voluntary public-private partnership to improve cybersecurity, and to strengthen cybersecurity research and development, workforce development and education, and public awareness and preparedness, and for other purposes" (US Congress, 2014). The Act directed NIST to "on an ongoing basis, facilitate and support the development of a voluntary, consensus-based, industry-led set of standards, guidelines, best practices, methodologies, procedures, and processes to cost-effectively reduce cyber risks to critical infrastructure" (US Congress, 2014). NIST is, as of this writing, working on version 1.1 of cybersecurity framework. Draft version 1.1 was released on January 10, 2017, based on feedback received on version 1.0 and comments received at an NIST-sponsored workshop in April 2016. The main updates to version 1.0 are the following:

- The addition of a section on measuring cybersecurity effectiveness
- An expansion on the use of the cybersecurity framework for cybersupply chain risk management
- Improvements in the access control category related to authentication, authorization, and identity proofing
- Improved explanation of the relationship between tiers and profiles

NIST intends to publish the final of version 1.1 in the fall of 2017.

The cybersecurity framework is a voluntary framework available to everyone within and outside the United States. Among its benefits, it provides a common language and framework for cybersecurity discussion that will hopefully foster communication between the public and private sector as well as among all organizations interested in improving cybersecurity. The cybersecurity framework is in use by organizations around the world and may become the de facto standard for measuring and improving the cybersecurity posture of organizations.

To promote the usage of the cybersecurity framework within the US Government, on May 11, 2017, President Trump issued an EO directing US Government executive branch agencies to use the cybersecurity framework "to manage the agency's cybersecurity risk" (White House, 2017). This EO requires agencies to provide a written action plan to the executive branch on how the agency will implement the cybersecurity framework and align the agency's policy, guidelines, and standards with the cybersecurity framework. The action plans are not required until after the deadline for this book, but it is hoped that having the entire US Government executive branch using the cybersecurity framework to implement its cybersecurity risk management and cybersecurity plans will provide a significant quantity of real-life actionable lessons learned and feedback on the cybersecurity framework. NIST can, per its authority under the Cybersecurity Enhancement Act of 2014, use this data to further evolve and improve the cybersecurity framework to address the ever-evolving threat landscape. Such an effort can only benefit the cybersecurity community at large.

So while the US Government has not passed any general-purpose cybersecurity and privacy laws or regulations, EOs directing the creation and usage of the cybersecurity framework and the Cybersecurity Enhancement Act of 2014, which directs NIST to continuously facilitate and support cybersecurity efforts, have produced an actionable and evolving framework that will hopefully help any type of organization implement, measure progress, and improve their own cybersecurity efforts.

14.2.2 Compliance/audits

Even if well-defined general-purpose US cybersecurity regulations were in place, organizations would still want assurances that their service providers are taking due care in safeguarding the sensitive, business critical information that the service provider is processing and/or storing for the organization. To provide this assurance, several industry and technical groups have come up with compliance standards and defined audit regimes so that service providers can provide third-party attestation that they take due care with the information/data entrusted to them.

Following is an overview of some of the more well-known and utilized compliance and audit regimes. This is by no means an exhaustive list and service providers should listen to their customers to determine the specific regime(s) that a service provider's customers would like them to follow. These compliance mechanisms may be built into a company's protocols via company policy, via contractual commitment with a customer or other third party, or more informally done as needed. Each standard involves reporting, internal or external as required, and ideally, follow-up actions to assure continuing compliance.

14.2.2.1 American Institute of Certified Public Accountants system and organization controls

The American Institute of Certified Public Accountants has defined a set of system and organization controls (SOC) service offerings that allow the system-level controls of a service organization or the entity-level controls of other organizations to be audited by certified public accountants (CPAs). The reports that an organization can have a CPA firm provide are the following:

- SOC 1—SOC for services organizations: internal controls over financial reporting (ICFR)

  A SOC 1 report covers ICFR, which are controls that the service provider has in place to protect their customer's data that would have an effect on the customer's

own controls for their financial reporting. The service provider's customer and the customer's CPA use these reports to evaluate the service provider's controls that affect the customer's financial reports.

- SOC 2—SOC for services organizations: trust services criteria

  SOC 2 reports cover the security, availability, and integrity of the systems the service provider uses to process their customer's data and the confidentiality and privacy of the data processed by these systems. These reports can be used by the service provider to monitor and measure progress on governance and risk management programs.
- SOC 3—SOC for services organizations: trust services criteria for general use report

  A SOC 3 report covers the same controls and scope as the SOC 2 report. They are written to be more widely disseminated and therefore do not contain the level of detail found in a SOC 2 report.

14.2.2.2 ISO/IEC 27000 series

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) are international organizations that work together through a joint committee to develop technical standards for IT. The ISO/IEC 27000 series (2017) provides background, common terminology, principles, techniques, and guidance on information security management systems (ISMSs). The main document in the ISO/IEC 27000 series is ISO/IEC 27001, officially titled "Information technology—Security techniques—Information security management systems—Requirements," was updated and rereleased in 2013. It describes what is required to implement an ISMS including understanding organizational context, required leadership support, risk assessment, and continuous improvement. The annex provides a list of security controls, grouped into 14 categories, that may, but are not required to, be used to implement the ISMS based on the risk assessment. Not requiring specific controls enables organizations to use a risk assessment methodology that makes the most sense for their business and still achieve compliance with ISO/IEC 27001.

ISO/IEC does not certify organizations as compliant with its standards. Certification is done by independent third-party organizations. Certifications are valid for 3 years after which a full renewal audit is required. The normal process is for an organization to have documentation and certification audits at the beginning of the 3-year cycle to ensure the ISMS is in place and properly documented followed by annual surveillance audits to check ongoing progress and operations at the beginning of years 2 and 3.

14.2.2.3 European Union's global data protection regulation

Last but not least in our discussion of cybersecurity standards is a look at the future of worldwide compliance. The European Union (EU)'s global data protection regulation (GDPR) (Trunomi, 2017) will take effect in 2018 and will have a significant effect on US businesses that operate in the EU, touch personal information of EU citizens, or simply do business on an international basis. While a full analysis of the potential impact of GDPR regulations on the security industry are beyond the scope of this chapter, suffice it to say that it will provide several cautionary tales for companies due to its high EU-based privacy standards, its comprehensive regulations, and its focus on monetary fines.

At this point, we return to the focus offered at the beginning of this chapter on the actual actors accomplishing the tasks laid out over the last few sections. Who are the people who implement each of these compliance goals and how do they interact with one another?

14.2.3 Navigating corporate structure, roles, and conflicts

The following positions reflect roles of individuals, their interactions with the corporate boards that govern companies, and potential conflicts as their responsibilities begin to overlap.

1. Executives: The role of those in the executive suite has been increased in recent years with a growing assignment of responsibility upward. In the past, IT was IT, and the technology side of the business stopped at the highest level with at most the CTO. Now the entire C-suite and executive-level personnel are expected to both understand and execute security protocols.
2. Cybersecurity lawyers, including in-house and outside counsel: Both inside and outside counsels for companies need to understand the basics of HIPAA, GLBA, and the GDPR, which is looming, at the time of this writing, for those organizations with EU customers in 2018.
3. IT personnel: Traditionally tasked with nearly all the work in this chapter save the most esoteric legal review, IT should now expand beyond educating its own to educating the C-level executives on what could and most likely will happen in the event of a major data breach. See, herein, the discussion of tabletop exercises, which give these parties an opportunity to interact and share knowledge on these issues.
4. Security and privacy professionals: A growing profession of security and privacy professionals has come up the ranks from a variety of backgrounds—IT, legal, employment/human relations (HR), and compliance professionals. Their role is to cross-pollinate among the other groups mentioned in this section, to make sure each group understands its role in cybersecurity. These are the individuals that design and run the tabletop exercises and prepare internal and external policies with input from the other stakeholders.
5. Marketing: Marketing and product design personnel get involved in privacy and data security at the very earliest stages of the process via a concept called privacy by design or security by design. These processes consider the regulations and laws that may apply to a new product or a new method of marketing the product and "bake in" the security and privacy protections rather than adding them as an overlay after the product is complete, or even launched. Marketing people also have a role to play in matching expectations about privacy and security with the reality of an Internet-connected device, including suggesting user-accessible privacy protections such as data input minimization and security self-help such as superior password design.
6. Investor relations: Reaching out to the investor community is the function of the investor relations team. Good security is a good business practice and may increase the value of the company or a particular product line with differentiated privacy protection.
7. Government relations: In addition to the rather specific function of working with government entities in a data breach scenario for notifications purposes, government relations personnel have a larger function to understand the motivations and expectations of a regulatory agency to prevent prosecutions or other negative attention on a more ongoing basis.
8. Customer care and call center managers: The first line of defense in a data breach or general concern about privacy and data security is the call center. The ability to scale up the customer response center in a disaster situation caused by humans (a hacking scenario) or by natural disasters (a flood taking out a data center) is key to security management.

9. HR management: As discussed in the education and training section, it is difficult to create a good security system in a company without creating a culture of security to support it. HR personnel are responsible for recruiting and background checks to decrease the likelihood of an insider attack and responsible for ongoing training about new regulations, new technologies, and newly creative ways of accessing the employer's network. Human-centered hacking, such as pretending to be someone with credentials or other methodologies that take advantage of human error or vulnerabilities are a particular focus of this team's expertise and creative efforts to protect data belonging to the company and to individual customers.
10. Cyberinsurance and risk management: Cyberinsurance is also discussed in this chapter, but here we focus on the individual personnel associated with choosing and implementing insurance and risk management techniques in the process. This group can enhance security by running through checklists embedded in risk management to avoid data loss and secure perimeters. Physical security, such as locking doors and checking badges, may be housed in the HR and/or risk management group.
11. Law enforcement and government contacts: Law enforcement, from the neighborhood police force to state attorneys general and federal agencies, not only have a specific role to play in the notification and investigation of a criminal hacking instance, but can also be brought in to educate employees or consumers about protecting privacy, avoiding fraud, and sidestepping identity theft bandits.
12. Auditors: Auditing has, for every intent and purpose, a financial meaning, a security meaning, and, increasingly, a privacy meaning as well. It can be used in internal policy practice to prevent security incidents and to assess the damage once a security incident has occurred. It may also appear in each or any of these contexts in the text of a B2B contract, with associated consequences for the companies in the event of a data breach.

14.2.4 Compliance activities conducted by personnel

14.2.4.1 Security/PIAs

PIAs and, in the EU, data DPIAs are, in a nutshell, a data audit of your company. Where are the data and how are they stored, transmitted, and processed? It is common to evaluate these issues internally and assign red, yellow, or green colors to each existing practice to evaluate whether they are dangerous, questionable, or just fine as is. The next step is to research industry standards and get each category up to speed. See the section in this chapter on security standards for details on how to accomplish this task. While security audits and evaluations are, as discussed herein, quite detailed and standardized, the privacy industry has more variance in its ability to assess how much privacy is available to individuals. PIAs can incorporate security standards and build upon them to provide assurances to business partners, consumers, and government officials that privacy is an important part of the protocols of a company.

14.2.4.2 Tabletop exercises

A tabletop exercise is exactly what it sounds like—there is a group of people sitting around a table, and an exercise, or rather a game, is played out over a period. Tabletop exercises get to the idea that in order to be prepared for a disaster, or even a minor dilemma, it is best to run through various scenarios that may occur in advance of day zero. There is a variety of security incidents that could occur, from cables cut by vandals to national cybersecurity

meltdowns, but here we will go into some detail about two tabletop exercises that are worth spending some time outlining, and ideally, actually running.

1. Data breach hypothetical(s): The data breach hypothetical tabletop exercise requires a bit of imagination to posit some basic facts: Who or what caused this imaginary breach? How did we find out about it? What was the reaction of the media, the government and the individuals affected? Ultimately, the goal of the exercise is to create a checklist of items to review systems and procedures to avoid such a scenario from actually occurring.
2. Responses to class action lawsuits: A little less imagination is required here. One of the well-known class-action firms, or perhaps someone new to the game, files a suit against your company. What is the first thing that you do? Notify legal, but then what? Your tabletop exercise should run through the process of gathering a team to respond, including IT, legal, policy, investigations, media and customer relations personnel, and the head of any department involved in the security snafu. Investigate cautiously. Preserve necessary documents and processes under any litigation hold as instructed by counsel. Respond to media inquiries via a centralized point of contact and with prepared messaging.

14.2.4.3 Creating a corporate privacy culture

1. Internal policies: Internal policies for each company should include privacy policies (in addition to any legally required external privacy policy for customers) and security policies. They should be drafted within the parameters of industry standards discussed in this chapter and, when feasible, go beyond legal requirements to address forward-thinking security practices. The law is slow to incorporate new technologies, and even when legislators leap on a new technology, it takes some time for their ideas to become law.
2. Education and training: It does not do a company much good to have state-of-the-art security policies if no one is aware of them or follows them. Education designed to explain the meaning of each protocol, including the "whys" as well as the "shoulds," will disperse the knowledge in the IT and legal departments throughout the company. Training is the "how," i.e., once you have the requisite knowledge about company security practices, how does this apply to an individual employee's job and how can he/she pass on this knowledge to his/her reports and successors?
3. Resources for professionals: The International Association of Privacy Professionals, the Cloud Security Alliance, RSA, and Information Systems Audit and Control Association are several of the trade associations that offer resources for new and experienced privacy and data security professionals. Each of these organizations has a website with available resources, some of which are behind a paywall, and articles addressing current topics in privacy and security for professionals. They also offer live conferences and meetings during which individuals can confer on problems and solutions in the industry.

14.2.4.4 Contracts and security clauses

When designing a contract for the provision of tech services, the parties should begin with prevention and creating a secure interconnected network. This preliminary should create a structure of words that supports a company in avoiding a data breach or security incident and mitigate the effects of a data breach. The contract is that framework, and

the lawyers, IT professionals, and security personnel are each a piece of the puzzle with support and information gathering from engineering and then sharing/training after the contract is signed.

Following are factors to examine when evaluating the efficacy of security and data breach clauses in protecting each company involved in a transaction from not only the likelihood of breach, but also the resulting rather enormous liability consequences of breach. First, consider the relative sophistication of parties. Are the parties equally situated with regard to technological sophistication and experience? In some situations, the answer may well be yes, the parties are both technology providers, as in a transaction between a software manufacturer and an enterprise-level telecommunications company. In other instances, the companies may be divergent, for example, a cloud storage company serving a small chain of pizza restaurants. Next, evaluate the control of data by each company. Again, there may be widely different levels of ability to control data based on the type of services being offered in the contract. In a true outsourcing arrangement, one party controls nearly all the other party's data. In many cases, IT personnel will need to explain to management whether they truly have access to the data versus the mere possibility of access, from an accidental or intentional breach of access protocols. Also, the types of use of data should be factored in, including data storage or data processing, each of which entails different risk protocols when the data are in transit (often encrypted) and then when the data are at rest, preferably behind a network security firewall and physical security protections. Finally, does one or more parties have data security or breach insurance and/or access to availability of insurance? Some parties will sidestep the issue of insurance by representing that they have self-insurance, i.e., deep pockets.

14.2.4.5 Legal negotiation strategy for data breach and data security

There are several factors that can throw a wrench in negotiations, even if the parties agree on the basic plan to increase mutual data security and avoid data breaches if possible:

1. Definitions: Most contracts begin with a definitions section. One tricky definition to create is the definition of a data breach. For example, most security professionals will acknowledge that security incidents are subbreach. Some level of security incident occurs all the time, and it matters quite a bit when they roll over into a "data breach" as defined by the contract or the law. Several state laws have minimum requirements for data breach by defining the number of affected individuals or state citizens and have another trigger for encrypted versus unencrypted data.
2. Legislation: New legislation is always being proposed, especially in the media noteworthy areas of data breach, individual privacy, and national security as it applies to private companies. Many corporations would kill for comprehensive data breach legislation as long as they can write it themselves. As a matter of practicality, most legislators do not have either the expertise or the time to write highly technical bills and often rely on industry experts to draft portions of the legislation that relate to data security. As a result, the draft usually winds up touting best practices or industry standards or another somewhat vague standard if you do not have the context of interpretative case law or contracts in hand with detailed attachments outlining security requirements. This situation leads to full employment for lawyers to interpret and litigate over the enacted laws and regulation. Further complicating the legislative issue is the multiple jurisdictions that may be jockeying for position on the issue of data security. This also requires legal interpretation, both on a general level

and specific to any given deal. For example, a law firm may provide not just ad hoc advice, but an interactive tool to juxtapose regulations in multiple jurisdictions. If at some point after this writing we see an enacted federal legislation on the issue of data security, the law will likely, in order to avoid an unending battle of wills, still exempt state laws. That leaves 51 potential jurisdictions, including Puerto Rico, Washington DC, Guam, as well as the financial and healthcare sectoral regulations, to push around the parameters of the requirements.

3. Standing: Standing is the legal concept that whoever sues another must have a legal right to do so. Several recent cases in the privacy and data security area have begun looking at harm done as the threshold for standing to sue. The court decisions mention a requirement that there not just be hurt feelings as the result of a privacy violation, but that there must also be proof of some sort of financial harm to the affected individual in order for him/her to have standing to sue. It is difficult to prove an increased risk of identity theft, but identity theft is nearly the only harm discussed in many of the cases. Identity theft protection is a marketed service, so there are damages associated with needing such protection as the result of having your personal data leaked to the public. Nevertheless, this is a small ticket item in comparison to the difficulties many individuals suffer as the result of being a victim of a data breach. In order to definitely provide compensation for such damages, some states may find a need for statutory damages, i.e., a set amount of compensation delivered to each victim regardless of proof of actual damages.
4. Departmental silos: The image of a grain or water silo tower standing tall and alone in the field is a vivid one, and it accurately represents the idea that large companies have different departments for each functionality, and the departments often do not communicate with each other often or well. There may be different legal departments even for privacy and for security issues, or security operations may be housed in IT while privacy compliance is settled in with the regulatory group. While litigation seems like one department, issues that arise as the result of a company being targeted by class action lawsuit may find a different response than a privacy compliance matter that arises from an FTC enforcement action. Small companies may have no department to deal with privacy and security, and all issues must be defaulted to busy C-suite executives. Better business practices would be to designate a liaison to communicate policies among these departments. Also, as part and parcel of the training ideas espoused herein, all-hands calls and meetings can be used to educate each employee about his/her role in the company and its relation to the other roles in other departments. With these practices, silos may not be eliminated entirely, but at least everyone will be on the same page when an incident occurs.
5. Transparency: There is quite a bit of variation in how much is disclosed to the public about the internal security and privacy policies of a company. Privacy policies are generally public, whereas security policies are probably only public to the extent they are discussed in privacy policy or are offered as generalities about securing personal data to consumers. On a B2B level, companies will often allow highly sensitive data to be released under a higher level nondisclosure agreement. Highly sensitive data for a company would include trade secrets, network configuration maps, or proprietary and patent information. The ultimate transparency issue is an involuntary one—should we have a back door for encryption to enhance national security or would it decrease security because it opens up vulnerabilities?

14.2.4.6 Cyberinsurance

Cyberinsurance has enormously grown as an industry during the last few years. Still, it is not a mature complete product, and the statisticians are still working out the kinks. What can you legally and commercially obtain coverage for? The following discussion explores what is available and what to look for in a cyberinsurance policy. Starting with the obvious, a policy should cover basic security privacy and liability. Coverage amounts are still the big question. How much liability coverage would you need for a data breach? We know that California and other states have created or at least mirrored an industry standard for 12 months of identity theft protection for each affected individual/customer, plus the cost of customer and government notices and a wide variety of media interactions. Beyond data breach, consider insurance for a host of breach-related losses associated with business interruption, data recovery, regulatory procedure participation and compliance fines, and crisis management costs. A rising army of professionals can deal with each of these issues rather than having to divert internal operations to this crisis, but each item outsourced will have associated legal and business fees.

There are several cautionary tales associated with the insurance evaluation. It is worth noting that regular insurance ("commercial general liability" or CGL) will not cover this specialized loss. In addition, policies have exclusions for war or terrorism. Note that if you say that this is the reason for your breach or data loss, this may undermine your insurance coverage. The policy may have exclusions for vendors. The now infamous Target breach was likely the heating, ventilation, and air-conditioning vendor's fault, not a technology issue. The lesson here is to look at your coverage and investigate the source of the leak or breach before making a public statement.

What happens after you sign up for a cyberinsurance policy? Your work is not done. Next up is to flow down to subcontractors your security policies, review their policies and practices, or at least get representations and warranties from vendors. Contract language should limit vendors' access to data to a need-to-know basis, among other security precautions. Also, the legal counsel should lock in a flow down requirement to get cyberinsurance to any vendors/subcontractors on the deal, so the correct/liable party will be insured. As with any legal specialty, there are insurance-specific lawyers with expertise in these areas, and coverage lawyers can advise on types of insurance. Overall, consider any liability limitations in the policy, especially caps on policy. For example, even a rather generous $90 million policy may still not cover you if have $248 million in credit card losses as a big box retailer would suffer. Costs of cover for a data breach may include anything from simple customer notifications to elaborate data reconstruction/recreation. There are ancillary and consequential costs to the data breach, including post-contract monitoring, reporting, and auditing. All in all, be not overwhelmed by the choices and buy cyberinsurance or self-insure.

In the coming years, we will all become Carrie from *Homeland*. We will need to address cybersecurity in our daily lives, for our work and to protect our children. A basic understanding of how security and privacy are handled in the law, in technology, and in government policy will be useful for thriving in the coming cybercentury.

Bibliography

American Institute of CPAs, 2017, *System and Organization Controls—SOC Suite of Services*, http://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/SORHome.aspx.

Cornell Law School Legal Information Institute, 2017, 47 US Code § 222—Privacy of customer information, https://www.law.cornell.edu/uscode/text/47/222.

Harvard Law School Forum, 2017, *New York Cybersecurity Regulations for Financial Institutions Enter Into Effect*, https://corpgov.law.harvard.edu/2017/03/25/new-york-cybersecurity-regulations-for-financial-institutions-enter-into-effect/.
National Council of State Legislatures, 2017, *Security and Privacy*, http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-and-security.aspx.
Payment Card Industry Security Standards Council, 2017, Homepage, https://www.pcisecuritystandards.org/.
US Congress, 1999, S.900—*Gramm–Leach–Bliley Act*, https://www.congress.gov/bill/106th-congress/senate-bill/00900.
US Congress, 2014, S.2521—*Federal Information Security Modernization Act of 2014*, https://www.congress.gov/bill/113th-congress/senate-bill/2521.
US Federal Trade Commission, 2017, *Consumer Privacy*, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/consumer-privacy.
US National Institute of Standards and Technology, 2017, *NIST News*—NIST releases update to cybersecurity framework, https://www.nist.gov/news-events/news/2017/01/nist-releases-update-cybersecurity-framework.

References

HITRUST Alliance, 2017, *Understanding and Leveraging the CSF*, https://hitrustalliance.net/understanding-leveraging-csf/.
International Organization for Standardization, 2017, ISO/IEC 27000 Family—Information Security Management Systems, https://www.iso.org/isoiec-27001-information-security.html.
National Conference of State Legislatures, 2017, *States Laws Related to Internet Privacy*, http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx.
National Law Review, 2017, *State Data Breach Notification Laws*, http://www.natlawreview.com/article/state-data-breach-notification-laws-february-2017-privacy-update.
New York State Department of Financial Services, 2017, *Cybersecurity Requirement for Financial Services Companies*, http://www.dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf.
Payment Card Industry Security Standards Council, 2016, *PCI Data Security Standard Requirements and Security Assessment Procedures Version 3.2*, https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf [Must Accept PCI DSS Agreement to view document].
Trunomi, 2017, *EU GDPR Portal*, http://www.eugdpr.org/.
US Congress, 2014, *Cybersecurity Enhancement Act of 2014*, https://www.congress.gov/113/plaws/publ274/PLAW-113publ274.pdf.
US Department of Health and Human Services, 2017a, *The Security Rule*, https://www.hhs.gov/hipaa/for-professionals/security/index.html.
US Department of Health and Human Services, 2017b, *The Privacy Rule*, https://www.hhs.gov/hipaa/for-professionals/privacy/index.html.
US Department of Justice, 2017, *Privacy Act of 1974*, https://www.justice.gov/opcl/privacy-act-1974.
US DHS (US Department of Homeland Security), 2017, *About DHS*, See https://www.dhs.gov/about-dhs.
US FedRAMP, 2017, Program Overview, https://www.fedramp.gov/.
US FTC (US Federal Trade Commission), 2002, *How To Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act*, https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm.
US FTC, 2015, *Privacy and Security Update*, https://www.ftc.gov/reports/privacy-data-security-update-2015.
US Government Printing Office, 2011, 47 US Code § 222—Privacy of customer information, https://www.gpo.gov/fdsys/granule/USCODE-2011-title47/USCODE-2011-title47-chap5-subchapII-partI-sec222/content-detail.html.

US NIST (US National Institute of Standards and Technology), 2014, *Framework for Improving Critical Infrastructure Cybersecurity*, https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

US NIST, 2017, *FISMA Background*, http://csrc.nist.gov/groups/SMA/fisma/overview.html.

White House, 2013, Executive Order—Improving Critical Infrastructure Cybersecurity, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

White House, 2017, *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal.