A Guide to Defining Reasonable Cybersecurity

May 2024

CIS® Center for Internet Security®

CIS Controls™

Acknowledgements

CIS would like to recognize the following individuals and organizations for their support in creating this guide. Their time and expertise were a vital component of completing this important work.

Principal Authors

Aaron Charfoos, Paul Hastings LLP

Chris Cronin, HALOCK Security Labs

Brian de Vallance, Crosscut Consulting, LLC

Curtis Dukes, Center for Internet Security

Kirk M. Herath, CyberOhio, State of Ohio

Phyllis Lee, Center for Internet Security

Brian Ray, Leon M. and Gloria Plevin Professor of Law, Cleveland State University

Tony Sager, Center for Internet Security

Sharon Shoemaker, Center for Internet Security

Samuel A. Thumma, Phoenix, Arizona

Ira Victor, Chief Forensic Analyst, Discovery Technician

Community Reviewers and Contributors

Jennifer D. Bailey, Circuit Court Judge, Miami, FL (ret.)

Jay Billington, Center for Internet Security

Shay Cleary, National Center for State Courts

Rick Doten, VP, Information Security, Healthplan CISO, Centene

Steven Fugelsang, Program Director, Cybersecurity, National Governors Association

Casey Kennedy, Director, Information Services, Texas Office of Court Administration

Robin Regnier, Center for Internet Security

Contents

SECTION 1

Executive Summary

In the United States, there is no national, statutory, cross-sector minimum standard for information security.[1] No national law defines what would be considered *reasonable* security in matters involving data breaches. The federal and state governments have various statutes, regulations, policies, and caselaw covering elements of cybersecurity, like data breach notification and data privacy.

But all of these efforts fail to specify what an organization must do to meet the standard of *reasonable* cybersecurity.

The purpose of this guide is to do just that.

In collaboration with recognized technical cybersecurity and legal experts, the independent nonprofit Center for Internet Security® (CIS®) is publishing this guide to provide practical and specific guidance to organizations seeking to develop a cybersecurity program that satisfies the general standard of reasonable cybersecurity. This, in turn, could be a valuable resource to assist cybersecurity professionals, counselors, auditors, regulators, businesses, and consumers as well as lawyers and courts, in assessing whether an organization's program meets this same standard when the compromise of protected information gives rise to litigation or regulatory action. An equally important goal for publishing this guide is to reduce litigation resulting from data breaches. Building on laws and regulations currently in place, this guide identifies what is minimally adequate, absent express law governing the circumstances, for information security protections commensurate with the risk and magnitude of harm that could result from a data breach.

The authors of this guide considered federal and state laws, existing regulations, various industry best practices and cyber frameworks, and other resources to derive and propose a methodology for determining what should be considered reasonable cybersecurity to thwart data breaches. While there is no comprehensive U.S. law defining reasonable cybersecurity in all settings, this guide offers principles that may be used in interpreting and applying the laws that do exist.

Finally, this guide provides, as an example, how one framework, the CIS Critical Security Controls® (CIS Controls®)[2] can be implemented prescriptively, and in a manner that affords all those who use and rely on the technology ecosystem the ability to assess whether reasonable cybersecurity measures were taken.

SECTION 2

Introduction

"A data controller shall "[e]stablish, implement, and maintain *reasonable* administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data."

The Virginia Consumer Data Protection Act[3]

"What the HL Does Reasonable Data Security Really Mean?"**

Michael Buckbee[4]

Cybersecurity has rapidly moved from technical wizardry into the mainstream of risk-based decision-making for every enterprise. Rapid changes in complexity and connectivity also mean that individual enterprise decisions can affect the broader ecosystem. Therefore, even well-defined technical solutions must operate in a complex web of enterprise, economic, and social concerns to be effective.

Traditional cybersecurity frameworks have tried to bring order to this through large catalogs of technical and process controls, each supported by a wide variety of processes and certifications. However, there are dozens of these, each independently developed with good intentions in a specific context and ranging from voluntary to mandatory, descriptive to prescriptive, and sector-specific to general.

There is no national, statutory, cross-sector minimum standard of information security in the United States. No national law defines what would be considered reasonable security in matters involving data breaches. Given this lack of a national standard, negligence claims under the common law of the various states have become a frequent basis for data breach-related litigation. These types of common law negligence claims often require proving that the person or organization that caused the damage both had a legal obligation, i.e., owed a *duty of care* to the person claiming negligence, and failed to meet that obligation, i.e., exercise a *standard of care* that a reasonable person would provide.

In addition, all of the states have enacted cyber breach notification laws. Nearly 40% of the states have gone further in enacting data privacy laws that require reasonable cybersecurity. And six states have passed laws that help define reasonable cybersecurity.

In this complex environment, progress will require the convergence of technology, public policy, and economics. Laws and regulations are nearly unanimous in requiring that cybersecurity controls must be reasonable. By considering emerging state privacy and *safe harbor* laws as well as existing industry cybersecurity standards, this guide proposes that a definition for reasonable cybersecurity can be derived, articulated, and employed by using existing constructs from law and the cybersecurity community.

This guide further identifies that to support this convergence, cybersecurity standards must have specific properties, including demonstrated value against threats, be measurable, transparent, accessible, practical, and be supported by an ecosystem of tools and training. While existing esteemed studies and reports, such as the Sedona Conference Commentary on a Reasonable Security Test,[5] identified the need for cybersecurity standards, this guide goes further by describing the need for specific, prescriptive, and prioritized standards. The CIS Critical Security Controls is such a standard and is broadly applicable to the technical operations of any organization. In addition, the CIS Controls are supported by a companion risk assessment method, CIS-RAM.[6] CIS-RAM is accessible and practical for guiding an enterprise through the risk decision-making process of implementing security controls (and the supporting actions, safeguards) to determine that the risk of harm to other parties is commensurate with the steps taken for risk reduction.

A determination of the reasonableness of cybersecurity controls serves multiple constituencies and must be meaningful to those communities. The laws mentioned above are a clear indicator that an enterprise's cybersecurity program must not only protect its organization but must provide reasonable cybersecurity to mitigate harm to others.

Regulators, to maintain public confidence and trust, must be able to articulate what their regulations mean when they demand reasonable safeguards. Litigators must be able to make clear arguments in the interest of their clients about reasonable practices without yielding to a confounding "battle of the experts." And perhaps most importantly, the public must have some standard to determine when an organization's actions and policies reflect an appropriate level of care in support of its legitimate purposes that serve the public. Leveraging the concepts in this guide addresses all these goals, with an additional intended outcome of reducing litigation.

SECTION 3

Summary of Current Cybersecurity Law in the United States

While a recent federal law requires critical infrastructure organizations to report cyber incidents to the Department of Homeland Security Cybersecurity and Infrastructure Security Agency (DHS CISA),[7] regulation of cybersecurity increasingly includes specific requirements for organizations in specific sectors, or for organizations that seek to do business with specific federal entities. As a result, federal regulation remains sector-based, inconsistent, and incomplete.

Meanwhile, every state in the U.S. requires organizations to notify affected individuals[8] and often regulators when a data breach occurs, and nearly 40% of the states have added requirements for covered entities to take proactive data security measures to protect personally identifiable information (PII). As mentioned earlier, six states point to specific industry best practices as reasonable security standards. While these state laws follow a similar trend toward increasingly specific requirements for cybersecurity, they likewise are incomplete and sometimes in conflict. In addition, state common law (that is, the body of law based on court decisions, rather than codes or statutes) is equally relevant to defining what reasonable means, and this differs state by state.

The following provides an abridged summary of the patchwork of federal and state laws and regulations existing today. Many of these laws have not been able to keep pace with the growth and complexity of technology and its use in society. Moreover, the reader will note that there is no clear and consistent guidance defining what constitutes reasonable cybersecurity.

Summary of Federal Law

Federal cybersecurity law in the United States has come in different forms at different times. Figure 1 displays an abridged summary of that patchwork of statutes and regulations. Further details about the federal requirements on this timeline can be found in Appendix K.

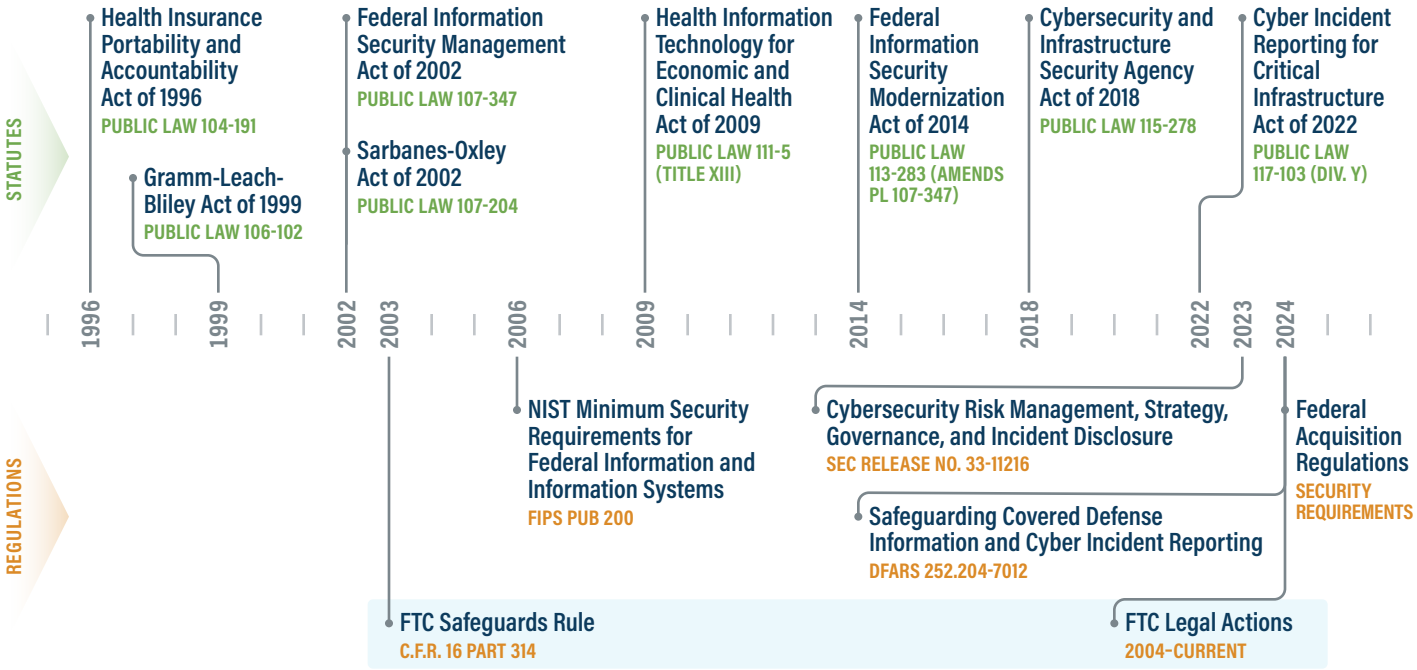
Summary of State Law

All 50 states plus the District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands have security breach notification laws that require organizations to notify consumers or citizens if their PII is breached.[9]

States increasingly have adopted specific data security laws or included data security requirements as part of broader consumer data privacy statutes. As mentioned above and noted in Appendices B and C, these laws, depicted in Figures 2 and 3, address the following categories of issues:

- General laws requiring broadly stated reasonable data security measures
- More prescriptive laws requiring organizations to develop, implement, and maintain specific data security measures, in some cases including specific controls and/or comprehensive written data security programs

Figure 1: Timeline of Federal Cybersecurity Law



- Comprehensive consumer data privacy laws that incorporate data security requirements, often broadly stated reasonable security but in some cases more specific requirements

- Safe harbor laws that provide incentives for organizations to adopt comprehensive data security programs. They permit companies to assert, for example, an affirmative defense or limit punitive damages in cybersecurity litigation where the company has implemented widely recognized and adopted cyber best practice standards, including National Institute of Standards and Technology (NIST) Cybersecurity Framework and the CIS Controls

- Laws that target specific industries or activities, including connected device laws that impose specific data security requirements

At the time of publication of this guide, 19 states have enacted comprehensive data privacy or health data privacy statutes that each require organizations controlling private information to protect that data on their computer networks using reasonable security, but provide no criteria to achieve it. In addition, six states (some overlap with the above 19) have issued laws stating that following one of the industry frameworks expressly identified in the laws is conclusive evidence of reasonable cybersecurity. Of those six, five are "Safe Harbor" laws that incentivize the voluntary adoption of certain cyber best practices. The sixth law, from Nevada, is a statute relating to personal information collected by governmental agencies. All of these six laws cite examples like the NIST Cybersecurity Framework or the CIS Critical Security Controls, although they do not require a specific framework nor direct how the frameworks should be interpreted or implemented to demonstrate due care. See Figures 2 and 3.

Apart from these statutory enactments, state executive branch regulations, and directives, decisions, and best-practice recommendations

Figure 2: State Comprehensive and Health Data Privacy Statutes

State Comprehensive Data Privacy Statutes

California. California Consumer Privacy Act as amended by the California Privacy Rights Act

Colorado. S. B. 21-190, Colorado Privacy Act

Connecticut. S. B. 6: Act Concerning Personal Data Privacy and Online Monitoring

Delaware. H. B. 154, Delaware Personal Data Privacy Act

Florida. S. B. 262, Florida Digital Bill of Rights

Indiana. S. B. 5, Consumer Data Protection

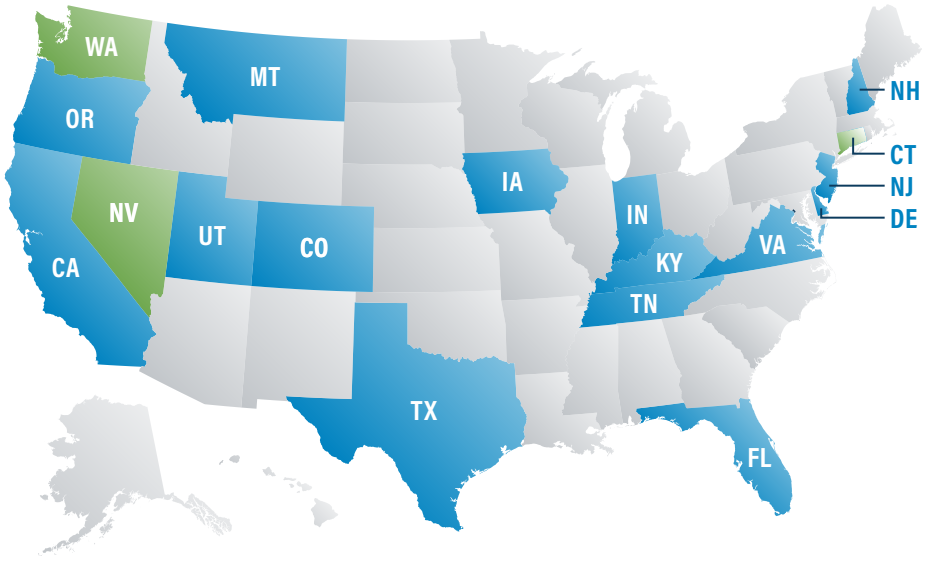
Iowa. S. F. 262, Consumer Data Protection Act

Kentucky. H. B. 15, Kentucky Consumer Data Protection Act

Montana. S. B. 384, Consumer Data Privacy Act

New Hampshire. S. B. 255, Consumer Expectation of Privacy.

New Jersey. S. 332, An Act Concerning Commercial Internet Websites, Consumers, and Personally Identifiable Information



Oregon. S. B. 619, Relating to Protections for the Personal Data of Consumers.

Tennessee. H. B. 1181, Tennessee Information Protection Act

Texas. H. B. 4, Texas Data Privacy and Security Act

Utah. S. B. 227, the Consumer Privacy Act

Virginia. Consumer Data Protection Act

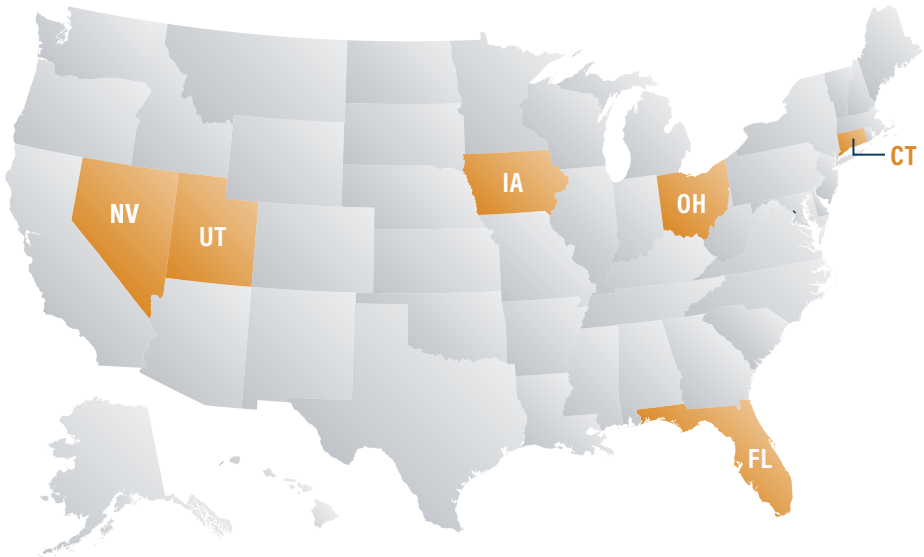
State Health Data Privacy Statutes

Connecticut. S. B. 3, An Act Concerning Online Privacy, Data and Safety Protections

Nevada. S. B. 370, Health Data Privacy Law

Washington. H. B. 1155, Washington My Health, My Data Act

Figure 3: States Leading the Way to Achieve Reasonable Cybersecurity



Connecticut. An Act Incentivizing the Adoption of Cybersecurity Standards for Businesses

Florida. Cybersecurity Incident Liability Act

Iowa. Affirmative Defenses for Entities Using Cybersecurity Programs

Nevada. State use of "reasonable security measures" to protect PII

Ohio. The Data Protection Act

Utah. The Cybersecurity Affirmative Defense Act

from other authorities, have become more common. A few examples are cited herein.

As one example, in 2009, Massachusetts enacted several substantive requirements for covered entities, including a written comprehensive information security program that contains administrative, technical, and physical controls.[10]

Another example is the cyber regulation of the New York Department of Financial Services (NYDFS). Effective November 1, 2023, NYDFS amended its existing cybersecurity regulations to further ensure that cybersecurity is integrated into regulated entities' business planning, decision-making, and ongoing risk management.[11] In particular, the new rules:

- Enhance governance requirements
- Require additional controls to prevent unauthorized access to information systems and to prevent or mitigate the spread of an attack
- Require more regular risk and vulnerability assessments, as well as stronger incident response and disaster recovery planning
- Update existing notification requirements, including a new requirement to report ransomware payments
- Update requirements for annual training and cybersecurity awareness programs.

As yet another example, in 2017, the Conference of State Bank Supervisors (a nationwide organization of banking and financial regulators) published its recommendations in a cybersecurity resource guide for bank executives, identifying industry-recognized standards for cybersecurity best practices currently used within the financial services industry and an organizational approach used by NIST.[12]

Even more recently, several states' attorneys general have entered into consent decrees with businesses that have experienced a breach. These voluntary compliance agreements provide that the company must develop, implement, and maintain a cybersecurity program designed to protect the security of the PII. See Appendix J for more details.

In civil litigation concerning data breaches, state common law tort claims generally include allegations that require proving that an organization failed to take reasonable measures to protect the compromised information. Usually, that means the plaintiff would hire a cybersecurity expert who would testify that what the company provided *was not reasonable* (i.e., was lacking some key security capabilities or practices), and the company, in turn, would hire its cybersecurity expert who would testify that what the company provided *was reasonable.*

While this growing area of law is moving in the direction of requiring more specific data security measures for some organizations in some contexts, organizations outside of those areas are still left with the challenge of identifying for themselves what constitutes reasonable cybersecurity. And, even in areas where state or federal law prescribes certain measures when faced with either litigation or a regulatory investigation, an organization must be able to articulate why the steps that it took (or did not take) to protect sensitive information were reasonable.

SECTION 4

Using Safe Harbor Statutes and Industry Frameworks to Define Reasonable Cybersecurity

"We expect that reasonable security measures will include measures that are commonly the subject of best practices."[13]

Federal Communication Commission

"In the absence of clear guidance from the courts, organizations must rely on a variety of sources to determine the reasonable standard of care in cybersecurity, including industry best practices, government regulations, and expert opinions."

James Lewis, Senior Vice President and Director of the Center for Strategic and International Studies

Organizations generally look inward to determine the impact of cybersecurity incidents involving the breached organization's better-understood and less-visible costs, including work disruptions, technical investigation, cybersecurity improvements, breach notifications, and post-breach consumer protections, as well as regulatory and recovery costs, fines, fees, and settlement payments.[14] They often forget to include in their risk analysis the harm they may cause others. (See Appendix I for a discussion of two methodologies to test for reasonable cybersecurity.)

States are beginning to point to solutions by identifying and accepting industry best practices and by referencing published frameworks as constituting reasonable security. The California Attorney General, in a Data Breach Report, concluded that failing to implement all relevant CIS Critical Security Controls "constitutes a lack of reasonable security."[15] Further, Nevada law requires state governmental agencies that maintain a resident's PII to implement and maintain reasonable security measures published by NIST or the Center for Internet Security concerning the collection, dissemination, and maintenance of records containing personal information.[16]

In addition, as summarized in Section 3, several states have passed safe harbor laws, which provide a similar way to identify reasonable cybersecurity. (See Appendix C for a list of these safe harbor statutes). Although differing on the margin, these safe harbor statutes follow a similar structure. Looking to the Ohio law, the progenitor of the safe harbor laws, as an example, its statute concludes that the scale and scope of a company's cybersecurity program "is appropriate if it is based on all of the following factors":[17]

- The size and complexity of the company
- The nature and scope of the activities of the company

- The sensitivity of the information to be protected
- The cost and availability of tools to improve information security and reduce vulnerabilities
- The resources available to the company

After identifying these five factors that help determine a scale and scope of an appropriate cyber defense, the Ohio safe harbor statute makes it even more clear for organizations by expressly accepting as reasonable those defenses based on:[18]

- The Framework for Improving Critical Infrastructure Cybersecurity developed by NIST
- NIST Special Publication 800-171
- NIST Special Publications 800-53 and 800-53a
- The Federal Risk and Authorization Management Program (FedRAMP) Security Assessment Framework
- The CIS Critical Security Controls
- The International Organization for Standardization/International Electrotechnical Commission (ISO) 27000 family – Information Security Management Systems

By listing factors that determine an appropriate scale and scope and then by expressly pointing to several specific, effective, existing industry best practices that will be deemed reasonable cybersecurity if followed, the Ohio safe harbor law creates a clear roadmap for organizations as they determine how best to mitigate risk.

Also, for organizations within particular industries, these safe harbor statutes provide sector-specific guidance concluding that a company is considered to have implemented reasonable security if it conforms to the current version of the applicable standards:[19]

- The security requirements of HIPAA
- Title V of the Gramm-Leach-Bliley Act
- FISMA as modified in 2014
- The Health Information Technology for Economic and Clinical Health Act
- The Payment Card Industry (PCI) data security standard

An important consideration is that these standards have active regulatory oversight and enforcement of the entities covered.

By identifying a set of more specific, prescriptive, and prioritized industry standards to guide organizations in developing cybersecurity programs, these laws could contribute to a clearer definition of what constitutes "reasonable" security more broadly, in other jurisdictions and other contexts outside of the areas in which the sectoral laws apply.

Where no specific sectoral standard or state regulation applies, the considerations outlined below can help better define reasonable cybersecurity.

While most of these frameworks provide relatively specific guidance for conducting assessments, they do not set a definitive standard for compliance. For example, NIST 800-53 emphasizes that compliance requires "using all appropriate information as part of an organization-wide risk management program" and the effective use of "the tailoring guidance and inherent flexibility in NIST publications so that the selected security controls documented in organizational security plans meet the mission and business requirements of organizations."[20] Implementing most of these standards in a given organization thus requires considerable expertise and the exercise of sound judgment.

The various frameworks mentioned and cited in this guide offer a range of prescriptive and flexible defensive actions an organization could take. Some are policy standards (e.g., NIST CSF). Some are data standards (e.g., PCI,[21] health care, ISO[22]). The CIS Controls, referenced in safe harbor and the Nevada statutes referenced throughout this paper, are *operational* standards. While there are other respected frameworks also mentioned, this guide considers the CIS Controls as an emerging, de-facto standard (see Appendix D). The following section focuses specifically on the CIS Controls and groups the Controls and their underlying, supporting actions into understandable categories to allow for more straightforward application. Readers wishing to focus on other frameworks are invited to review the framework mappings detailed in Appendix F.

SECTION 5

How an Organization Should Properly Implement Cyber Safeguards to Achieve Reasonable Cybersecurity

Organizational leaders should be asking themselves a basic set of questions regarding their cybersecurity health, including:

- What is the scope of our mission, obligations, and stakeholders?
- Do we know what is connected to our systems and networks?
- Do we know what is or is trying to run on our systems and networks?
- Do we understand the data that is running on our systems and the relative sensitivity?
- Are we limiting and managing the number of people who have privileges on our systems and networks?
- Have we established processes for reviewing the health of our networks, training employees, and recovering from possible breaches?
- What are our gaps and what risks do they pose?

In addressing these (and other) questions, organizations can show that they have established and actively maintain a cybersecurity program that includes protections commensurate with the risk and magnitude of harm that could result from a breach. One of the most effective ways to demonstrate this is by aligning with a known cybersecurity framework and measuring conformity and progress on the implementation of that framework's security criteria. Additionally, organizations must identify resources, perform periodic audits or assessments of their program (such as risk assessments and independent assessments for accuracy and sufficiency of the cybersecurity program), and address identified gaps. All these steps should be repeated as defined by the cybersecurity program. (See Appendix L for a Reasonableness Policy Checklist.)

There are multiple cybersecurity frameworks to choose from, and many of these frameworks provide credible security recommendations. Regardless of what cybersecurity framework an organization chooses, it is important to understand that "it's not just about the list (criteria)." Equally important is the ecosystem that supports the list. Organizations must be able to: get training, obtain implementation guidance from peers, measure progress or maturity, and show alignment with any required regulatory and compliance frameworks.
In this guide, we look to the CIS Critical Security Controls as providing guidance on how an organization should be able to show (and in states with statutory safe harbors, benefit from those safe harbors) reasonable cybersecurity measures. See Appendix D for why the CIS Controls are becoming a global de-facto standard. The CIS Controls are, quite intentionally, very detailed. In broad terms,

however, they can be broken into the following common-sense components:

1. know your environment
2. account and configuration management
3. security tools
4. data recovery
5. security awareness
6. business processes and outsourcing

See Appendix G for more detail.

The security controls applied to an enterprise must defend against and/or mitigate the effects of real-world attacks. Additionally, an organization must put in place additional controls and processes to respond and recover from an attack. These combined controls encompass reasonable security. (For a full description of prescriptive and prioritized activities that organizations should take to defend their enterprise, see Appendix H.)

Know Your Environment

The first thing an organization must do when implementing a cybersecurity framework is to "know your environment." An organization must know what assets (hardware and software) are on its network. They must also identify the data on the enterprise that they are obligated to protect. After doing this, to minimize their attack surface, an organization can prioritize the application of security controls to assets based on where high-value data resides.

Account and Configuration Management

Once an organization understands what assets exist in the enterprise environment, the next step is to perform account and configuration management. This includes defining the processes and rules for creating and revoking accounts and for determining what accesses various accounts have to system and enterprise resources. Such account governance is essential because a common attack vector includes compromising accounts and taking advantage of the access those accounts have on the network. (See Appendix E for a true case study.)

Another highly effective way to mitigate against and detect malicious activity is to apply and maintain a secure configuration across enterprise hardware and software assets. This includes network infrastructure. Enabling automated patching and keeping software up to date is a primary way in which organizations can defend against attacks. Also, configuring the collection and aggregation and requiring review of audit logs ensures organizations will analyze logs which helps with detecting and understanding an attack.

Security Tools

Commercial cybersecurity tools may be used to protect against common attacks, such as specific intrusions or malware. Malware can enter an organization through vulnerabilities within the enterprise on network infrastructure, end-user devices, email attachments, web pages, and more. This is why web browser and email protections are important for network defense. Organizations can deploy tools to prevent users from going to known, malicious websites and block malicious email attachments. Continuous monitoring through endpoint detection and response (EDR) is also important to defend against top threats. Additionally, host-based and network intrusion detection and prevention tools are critical to defend against security threats across the enterprise's infrastructure and user base.

Data Recovery

Given today's threat landscape, all organizations, regardless of size or industry, must put in place a data recovery plan as preparation for a breach. As such, best practices for recovering from and responding to an incident must be put in place. Organizations must implement a data recovery process that includes automated backups. Equally important is to establish a program to develop and maintain an incident response capability. At a minimum, organizations must identify roles and contact information for key personnel who are responsible for coordinating and responding to an incident.

Security Awareness

An effective cybersecurity program implements controls through people, processes, and technology. As such, an integral part of any cybersecurity program is security awareness education. This is the most effective defense against social engineering attacks, where threat actors impersonate a trusted source or trick users into clicking on a malicious link. Social engineering is also a popular attack vector for delivering ransomware. In addition to training, security awareness can also involve understanding how resistant your enterprise is to intrusions. Organizations can test the effectiveness of security controls by performing penetration testing and remediating vulnerabilities.

Business Processes and Outsourcing

Many organizations outsource their business processes. As such, organizations must develop processes to evaluate and manage service providers who are responsible for their sensitive data and functions. This includes inventorying, classifying, and assessing their providers.

Implementing these security best practices allows organizations to defend against top threats. Studies such as the *Verizon Data Breach Investigations Report*[23] and the Institute for Security and Technology's *Blueprint for Ransomware Defense: An Action Plan for Ransomware Mitigation, Response, and Recovery*[24] provide detailed evidence of this. For more information about the effectiveness of following such a framework, refer to Appendix H to find the implementation of the CIS Critical Security Controls and the underlying actions that support the Controls.

SECTION 6

Conclusion

In addressing reasonable cybersecurity measures, it is critically important for an organization to establish and sustain a cybersecurity program that balances the scope and complexity of implemented security controls against the risk and consequences of a data breach. This guide proposes that this can be accomplished by implementing the CIS Critical Security Controls (one of several known, referenced frameworks) and dividing that framework into sets of activities that can be applied to other frameworks. The concepts addressed here, and amplified in the appendices, provide a critical baseline to assist counselors, cybersecurity consultants, auditors, and regulators, as well as lawyers, litigants, and courts, in determining what constitutes reasonable security in matters involving data breaches.

APPENDIX A

Glossary

Administrator accounts

Dedicated accounts with escalated privileges used for managing aspects of a computer, domain, or the whole enterprise information technology infrastructure. Common administrator account subtypes include root accounts, local administrator and domain administrator accounts, and network or security appliance administrator accounts.

Application

A program, or group of programs, hosted on enterprise assets and designed for end-users. Applications are considered a software asset in this document. Examples include web, database, cloud-based, and mobile applications.

Authentication systems

A system or mechanism used to identify a user by associating an incoming request with a set of identifying credentials. The credentials provided are compared to those on a file in a database of the authorized user's information on a local operating system, user directory service, or within an authentication server. Examples of authentication systems can include active directory, multi-factor authentication (MFA), biometrics, and tokens.

Authorization systems

A system or mechanism used to determine access levels or user/client privileges related to system resources including files, services, computer programs, data, and application features. An authorization system grants or denies access to a resource based on the user's identity. Examples of authorization systems can include active directories, access control lists, and role-based access control lists.

CIS Controls

The CIS Critical Security Controls are a comprehensive set of 18 specific cybersecurity measures, or controls, to protect systems and manage cybersecurity risks. An individual CIS Control is a strategic-level best practice that is, in turn, supported by multiple CIS Safeguards. See, for example, CIS Control 3: Develop Processes and Technical Controls to Identify, Classify, Securely Handle, Retain, and Dispose of Data.

CIS Safeguard	A prescriptive technical or procedural security measure supporting a broader CIS Control to defend systems and data from cyber threats. Safeguards represent the actionable steps required for the proper implementation of a Control. Examples include documenting a data management process (3.1), securely disposing of data from all enterprise assets (3.5), and defining data sensitivity requirements (3.7).
Cybersecurity	Protecting systems, networks, and the information contained within those systems and networks from digital or electronic attacks.
Cybersecurity Risk Assessment	The process by which risks are identified and the impact of those risks determined.
Database	Organized collection of data, generally stored and accessed electronically from a computer system. Databases can reside remotely or on-site. Database Management Systems (DMSs) are used to administer databases and are not considered part of a database for this document.
Data Privacy	The subset of data security activities to ensure data is only available to those who have authorized access to it.
Data Security	Protecting data (i.e., information: personal data, operational data, and system data) from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability of that data. (Analogous to information security). Sometimes, the definition also includes protection of the systems and networks on which the data resides.
Duty of care, Standard of care, Due care	Duty of care is a legal obligation to avoid actions or omissions that could foreseeably harm others. Standard of care is the specific level of care that is expected under the duty of care. It is often measured by the actions of an ordinarily reasonable person in similar circumstances. Due care is a term for fulfilling the standard of care that means acting with the necessary caution to avoid foreseeable risks. Due care is often referred to as “ordinary care” or “reasonable care” and is a benchmark to assess if a duty of care has been breached.

Ecosystem	Processes, information, and support related to and underpinning a particular topic or activity.
End-user devices	Information technology (IT) assets used among members of an enterprise during work, off-hours, or any other purpose. End-user devices include mobile and portable devices such as laptops, smartphones, and tablets, as well as desktops and workstations. For this document, end-user devices are a subset of enterprise assets.
Enterprise assets	Assets with the potential to store or process data. For the purpose of this document, enterprise assets include end-user devices, network devices, non-computing/Internet of Things (IoT) devices, and servers, in virtual, cloud-based, and physical environments.
Externally-exposed enterprise assets	Refers to enterprise assets that are public facing and discoverable through domain name system reconnaissance and network scanning from the public internet outside of the enterprise's network.
Information security	See Data Security. In earlier vernacular, this term referred to ensuring the availability, integrity, and confidentiality of electronic systems and their data.
Internal enterprise assets	Refers to non-public facing enterprise assets that can only be identified through network scans and reconnaissance from within an enterprise's network through authorized authenticated or unauthenticated access.
Library	Pre-written code, classes, procedures, scripts, configuration data, and more, used to develop software programs and applications. It is designed to assist both the programmer and the programming language compiler in building and executing software.
Network devices	Electronic devices required for communication and interaction between devices on a computer network. Network devices include wireless access points, firewalls, physical/virtual gateways, routers, and switches. These devices consist of physical hardware, as well as virtual and cloud-based devices. For the purpose of this document, network devices are a subset of enterprise assets.

Network infrastructure	Refers to all of the resources of a network that make network or internet connectivity, management, business operations, and communication possible. It consists of hardware and software, systems and devices, and it enables computing and communication between users, services, applications, and processes. Network infrastructure can be cloud, physical, or virtual.
Operating system	System software on enterprise assets that manages computer hardware and software resources and provides common services for programs. Operating systems are considered a software asset and can be single- and multi-tasking, single- and multi-user, distributed, templated, embedded, real-time, and library.
Personally identifiable information (PII)	Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual, NIST SP 800-63-3.
Physical environment	Physical hardware parts that make up a network, including cables and routers. The hardware is required for communication and interaction between devices on a network.
Reasonable cybersecurity	Measures that are intended to protect against the loss, misuse, or unauthorized access to, or modification of, information or data based on the appropriate standard of care of how a reasonably prudent person in the same or similar circumstances would act. Considerations include but are not limited to the: ▪ Size and complexity of the organization ▪ Nature and scope of the activities of the organization ▪ Sensitivity of the information to be protected ▪ Cost and availability of tools to improve information security and reduce vulnerabilities ▪ Resources available to the organization Some state laws expressly state that implementing specifically identified industry best practices constitutes reasonable cybersecurity.

Remote devices	Any enterprise asset capable of connecting to a network remotely, usually from the public internet. This can include enterprise assets such as end-user devices, network devices, non-computing/ Internet of Things (IoT) devices, and servers.
Servers	A device or system that provides resources, data, services, or programs to other devices on either a local area network or a wide area network. Servers can provide resources and use them from another system at the same time. Examples include web servers, application servers, mail servers, and file servers.
Service accounts	A dedicated account with escalated privileges used for running applications and other processes. Service accounts may also be created just to own data and configuration files. They are not intended to be used by people, except for performing administrative operations.
Services	Refers to a software functionality or a set of software functionalities, such as the retrieval of specified information or the execution of a set of operations. Services provide a mechanism to enable access to one or more capabilities, where the access is provided using a prescribed interface and based on the identity of the requestor per the enterprise's usage policies.
Social engineering	Refers to a broad range of malicious activities accomplished through human interactions on various platforms, such as email or phone. It relies on psychological manipulation to trick users into making security mistakes or giving away sensitive information.
Software assets	Also referred to as software in this document, are the programs and other operating information used within an enterprise asset. Software assets include operating systems and applications.
User accounts	An identity created for a person in a computer or computing system. For this document, user accounts refer to "standard" or "interactive" user accounts with limited privileges and are used for general tasks such as reading email and surfing the web. User accounts with escalated privileges are covered under administrator accounts.

APPENDIX B

State Data Privacy Statutes

State Comprehensive Data Privacy Statutes

The following 16 U.S. states have adopted comprehensive data privacy statutes. Comprehensive data privacy laws provide rights to consumers such as the right to access, correct inaccuracies in, delete, obtain a copy of, and opt out of the processing of their personal data held by entities not covered under specific sectorial laws. They also make requirements of the controller such as requiring reasonable protection of data and reasonable purpose in processing.

Kentucky: H. B. 15, Kentucky Consumer Data Protection Act

- **Overview:** This is a comprehensive data privacy law. This act does not provide a private right of action.
- **Status:** The Governor signed into law on April 4, 2024. Effective date: Jan 1, 2026.
- **Link:** https://apps.legislature.ky.gov/record/24RS/hb15.html

New Hampshire: S. B. 255, Consumer Expectation of Privacy.

- **Overview:** This is a comprehensive data privacy law. This act does not provide a private right of action.
- **Status:** The Governor signed into law on March 6, 2024. Effective date: Jan 1, 2025
- **Link:** https://gencourt.state.nh.us/bill_status/billinfo.aspx?id=865&inflect=1

New Jersey: S. 332, An Act Concerning Commercial Internet Websites, Consumers, and Personally Identifiable Information

- **Overview:** This is a comprehensive data privacy law. This act does not provide a private right of action.
- **Status:** The Governor signed into law on January 16, 2024. Effective date: Jan 16, 2025
- **Link:** https://www.njleg.state.nj.us/bill-search/2022/S332

Delaware: H. B. 154, Delaware Personal Data Privacy Act

- **Overview:** This is a comprehensive data privacy law. This act does not provide a private right of action.
- **Status:** Effective date: Jan 1, 2025
- **Link:** https://legis.delaware.gov/BillDetail/140388

Oregon: S. B. 619, Relating to Protections for the Personal Data of Consumers.

- **Overview:** This is a comprehensive data privacy law. This act does not provide a private right of action.
- **Status:** The Governor signed into law on July 18, 2023. Effective date: July 1, 2024.
- **Link:** https://olis.oregonlegislature.gov/liz/2023R1/Measures/Overview/SB619

Texas: H. B. 4, Texas Data Privacy and Security Act

- **Overview:** This is a comprehensive data privacy law. This act does not provide a private right of action.
- **Status:** The Governor signed into law on June 18, 2023. Effective date: July 1, 2024.
- **Link:** https://capitol.texas.gov/BillLookup/History.aspx?LegSess=88R&Bill=HB4

Florida: S. B. 262, Florida Digital Bill of Rights

- **Overview:** Some do not consider this a comprehensive data privacy law because its scope is limited by its definition of "controller," however this act provides the same rights to consumers and responsibilities for controllers. For the act to apply, a controller must be a for-profit entity that generates more than $1 billion in annual revenue and either make at least 50% of that revenue from the sale of online advertisements, "[o]perate[] a consumer smart speaker and voice command component service with an integrated virtual assistant connected to a cloud computing service that uses hands-free verbal activation," or operate an app store or similar platform with at least 250,000 apps. This act does not provide a private right of action.
- **Status:** The Governor signed into law on June 6, 2023. Effective date: July 1, 2024.
- **Link:** https://www.flsenate.gov/Session/Bill/2023/262/

Montana: S. B. 384, Consumer Data Privacy Act

- **Overview:** This is a comprehensive data privacy law. This act does not provide a private right of action.
- **Status:** The Governor signed into law on May 19, 2023. Effective date: Oct 1, 2024.
- **Link:** https://leg.mt.gov/bills/2023/billpdf/SB0384.pdf

Tennessee: H. B. 1181, Tennessee Information Protection Act

- **Overview:** This is a comprehensive data privacy law. This act does not provide a private right of action.
- **Status:** The Governor signed into law on May 11, 2023. Effective date: July 1, 2025.
- **Link:** https://wapp.capitol.tn.gov/apps/BillInfo/Default.aspx?BillNumber=HB1181

Indiana: S. B. 5, Consumer Data Protection

- **Overview:** This is a comprehensive data privacy law. This act does not provide a private right of action.
- **Status:** The Governor signed into law on May 1, 2023. Effective date: Jan 1, 2026.
- **Link:** https://iga.in.gov/legislative/2023/bills/senate/5

Iowa: S. F. 262, Consumer Data Protection Act

- **Overview:** This is a comprehensive data privacy law. This act does not provide a private right of action.
- **Status:** The Governor signed into law on Mar. 28, 2023. Effective date: Jan 1, 2025.
- **Link:** https://www.legis.iowa.gov/legislation/BillBook?ga=90&ba=sf262

Connecticut: S. B. 6: Act Concerning Personal Data Privacy and Online Monitoring

- **Overview:** Before this law came into effect, Connecticut already had a comprehensive data privacy law providing consumers with certain rights and imposing responsibilities on controllers, with respect to health data.
- **Status:** The Governor signed into law on May 10, 2022. Effective date: Jan 1, 2023.
- **Link:** https://www.cga.ct.gov/2022/ACT/PA/PDF/2022PA-00015-R00SB-00006-PA.PDF

Utah: S. B. 227, the Consumer Privacy Act

- **Overview:** This is a comprehensive data privacy law. This act does not provide a private right of action.
- **Status:** The Governor signed into law on Mar 24, 2022. Effective date: Dec 31, 2023.
- **Link:** https://le.utah.gov/~2022/bills/static/SB0227.html

Colorado: S. B. 21-190, Colorado Privacy Act

- **Overview:** This is a comprehensive data privacy law. This act does not provide a private right of action.
- **Status:** The Governor signed into law on July 7, 2021. Effective date: July 1, 2023.
- **Link:** https://leg.colorado.gov/bills/sb21-190

Virginia: Consumer Data Protection Act

- **Overview:** This is a comprehensive data privacy law. This act does not provide a private right of action.
- **Status:** Effective date: Jan. 1, 2023.
- **Link:** https://law.lis.virginia.gov/vacodefull/title59.1/chapter53/

California: California Consumer Privacy Act as amended by the California Privacy Rights Act

- **Overview:** This is a comprehensive data privacy law. The California Consumer Privacy Act provided many of the rights and requirements of a comprehensive data privacy law and was amended by the California Privacy Rights Act to become fully comprehensive with provisions such as the right to correct inaccuracies in collected personal data. This act does not provide a private right of action.
- **Status:** California Consumer Privacy Act (effective Jan. 1, 2020), California Privacy Rights Act (fully effective Jan . 1, 2023).
- **Link:** https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

State Health Data Privacy Statutes

In addition, the following three states have passed data privacy laws that only apply to health data. These laws provide similar rights to consumers and similar responsibilities for controllers as the comprehensive data privacy laws, however, they only apply to the health sector. These laws also prohibit controllers from selling health data and require them to obtain consent to collect data.

Connecticut: S. B. 3, An Act Concerning Online Privacy, Data and Safety Protections

- **Overview:** Before this law came into effect, Connecticut already had a comprehensive data privacy law providing consumers with certain rights and imposing responsibilities on controllers, with respect to health data. As such, this law only adds the provisions of a health data privacy law that are not already included in a comprehensive data privacy law, such as prohibiting controllers from selling health data and requiring them to obtain consent to collect data.
- **Status:** The Governor signed into law on June 26, 2023. Effective date: July 1, 2023.
- **Link:** https://www.cga.ct.gov/asp/cgabillstatus/cgabillstatus.asp?selBillType=Bill&bill_num=SB00003&which_year=2023

Nevada: S. B. 370, Health Data Privacy Law

- **Overview:** This is a health data privacy law.
- **Status:** The Governor signed into law on June 15, 2023. Effective date: Mar 31, 2024.
- **Link:** https://www.leg.state.nv.us/App/NELIS/REL/82nd2023/Bill/10323/Overview

Washington: H. B. 1155, Washington My Health, My Data Act

- **Overview:** This is a health data privacy law.
- **Status:** The Governor signed into law on Apr 27, 2023. Effective date: July 23, 2023.
- **Link:** https://app.leg.wa.gov/billsummary?BillNumber=1155&Year=2023&Initiative=false

APPENDIX C

States Leading the Way to Achieve Reasonable Cybersecurity

Several states have passed laws that provide a way to identify reasonable security. The following six states have enacted statutes that incentivize the voluntary adoption of cyber best practices by creating a safe harbor for organizations that adopt one of several industry standards, like the CIS Critical Security Controls. These states include:

Florida: Cybersecurity Incident Liability Act

- **Overview:** Incentivizes voluntary adoption of cybersecurity best practices, including the CIS Critical Security Controls, by providing that organizations are not liable in connection with a cybersecurity incident if they have implemented these standards. Also, the law provides that certain failures are not evidence of negligence and do not constitute negligence per se and further specifies that the defendant in certain actions has a certain burden of proof. The law additionally provides that a county, municipality, or other political subdivision of the state that substantially complies with the cybersecurity training, standards, and notification protocols under current law is not liable in connection with a cybersecurity incident.
- **Status:** Passed the legislature on March 5, 2024, and, as of the date of this publication, is awaiting signature by the governor. Effective date: When signed by the governor.
- **Link:** Legislative history of HB 473 - Cybersecurity Incident Liability, including link to enrolled bill text: https://www.myfloridahouse.gov/Sections/Bills/billsdetail.aspx?BillId=79076

Iowa: Affirmative Defenses for Entities Using Cybersecurity Programs

- **Overview:** Incentivizes voluntary adoption of cybersecurity best practices, including the CIS Critical Security Controls, by creating affirmative defenses in a lawsuit resulting from a data breach.
- **Status:** Effective date: July 1, 2023.
- **Link:** Iowa Code Title XIII (Commerce), Chapter 554G (Tort Liability—Cybersecurity Programs. https://www.legis.iowa.gov/law/iowaCode/sections?codeChapter=554G&year=2024

Connecticut: An Act Incentivizing the Adoption of Cybersecurity Standards for Businesses

- **Overview:** Incentivizes voluntary adoption of cybersecurity best practices, including the CIS Critical Security Controls, by creating a cap against punitive damages in a lawsuit resulting from a data breach.
- **Status:** Effective date: October 1, 2021.
- **Link:** Public Act No. 21-119. https://www.cga.ct.gov/2021/ACT/PA/PDF/2021PA-00119-R00HB-06607-PA.PDF

Utah: The Cybersecurity Affirmative Defense Act

- **Overview:** Incentivizes voluntary adoption of cybersecurity best practices, including the CIS Critical Security Controls, by creating an affirmative defense against lawsuits resulting from a data breach.
- **Status:** Effective date: May 5, 2021.
- **Link:** Utah Code Title 78B (Judicial Code), Chapter 4 (Limitations on Liability), Part 7 (Cybersecurity Affirmative Defense Act) (effective 5/5/2021): https://le.utah.gov/xcode/Title78B/Chapter4/C78B-4-P7_2021050520210505.pdf

Nevada: State use of "reasonable security measures" to protect PII

- **Overview:** Requires that state data collectors comply with the CIS Critical Security Controls or the NIST Cybersecurity Framework concerning the collection, dissemination, and maintenance of records containing personal information of a resident of Nevada.
- **Status:** Effective date: January 1, 2021.
- **Link:** S.B. 302, Chapter 412: https://www.leg.state.nv.us/App/NELIS/REL/80th2019/Bill/6534/Overview

Ohio: The Data Protection Act

- **Overview:** Incentivizes voluntary adoption of cybersecurity best practices, including the CIS Critical Security Controls, by creating an affirmative defense against lawsuits resulting from a data breach.
- **Status:** Effective date: November 1, 2018.
- **Link:** Senate Bill 220, codified at O.R.C. §§ 1354.01-1354.05: http://codes.ohio.gov/orc/1354

APPENDIX D

Why the CIS Critical Security Controls are Becoming a Global De Facto Standard

While there are some limited *policy* standards (e.g., NIST CSF) and industry or *data* standards (e.g., PCI, HIPAA, & ISO), there are no specific *operational* standards across all the economic sectors. The CIS Critical Security Controls are becoming the de facto, global reasonable standard for operational cybersecurity for six compelling reasons.

1 **Prescriptive and prioritized by global experts.** The CIS Controls, which are regularly compiled by cybersecurity experts around the world, help implement the goals of the NIST CSF by providing a blueprint for network operators to improve cybersecurity by identifying specific, prescriptive actions to be done in priority order based on the current state of the global cyber threat. While the NIST CSF is the *what*—NIST defines the categories of cybersecurity and an organizational view of security risk management—the CIS Controls are devised based on *how* malicious actors attack and are updated regularly. What results is the clearest, most definitive roadmap of how to protect an organization from cyber attacks.

2 **Extremely effective and measurable.** The CIS Controls are very effective against today's most pervasive attack vectors and this effectiveness has been quantified. CIS's Community Defense Model (CDM) establishes that the CIS Controls mitigate approximately 86% of attack techniques found in the MITRE ATT&CK Framework.[25]

3 **Scalable.** The CIS Controls can be tailored by the size of the implementing organization. The CIS Controls introduce the concept of Implementation Groups (IGs), which provide both an onramp for organizations just starting out as well as a roadmap to greater cyber defense maturity by offering three tiers. These IGs tailor the controls to the size and maturity of the implementing organization. Even at the simplest level, IG1, the CIS Controls remain very effective, protecting against 74% of attack vectors identified in the MITRE ATT&CK model.[26]

4 **Cost-effective.** Recognizing that cost of implementation is a huge unknown in security programs (especially for small- and medium-enterprises), CIS has been developing tools, models, and working aids to help enterprises understand and manage the cost of their cybersecurity program. For example, the CDM establishes the "security value" of individual practices,[27] which assists in priority-setting and also bounds the costing question to specific practices and tools. It also helps enterprises establish the baseline value of technology and practices that they already have. Further, CIS has also published a study to establish how much it will cost an organization to implement effective cybersecurity.[28]

5 Mapped to other global policy and data frameworks. The CIS Controls are mapped to many existing frameworks.[29] Many enterprises must report progress against multiple security frameworks or sets of requirements, and so CIS develops freely available, industry-vetted mappings to and from CIS products to all major security frameworks (like the NIST CSF, NIST 800-53, PCI, etc.) This framework mapping is also available in Appendix F.

6 Widely adopted globally.

- The CIS Critical Security Controls have been downloaded over 400,000 times over the last few years—over half of these by organizations outside the U.S.
- Selected adoption and endorsements of the CIS Critical Security Controls include:
  - **NIST, "Framework for Improving Critical Infrastructure Cybersecurity Framework," Version 1.1, Apr 16, 2018.** Cites and maps to "CIS CSC" throughout Appendix A, Framework Core at 22-44. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf The "CIS CSC" is a shorthand for the CIS Critical Security Controls, also referred to as the CIS Controls throughout this paper.
  - **Verizon, "DBIR Data Breach Investigations Report," 2024.** Recommends the CIS Controls and maps them to industry challenges and vulnerabilities. https://www.verizon.com/business/resources/reports/dbir/
  - **National Aerospace Standard, NAS9933, Critical Security Controls for Effective Capability in Cyber Defense, Nov. 29, 2018.** Based on the CIS Controls. https://store.accuristech.com/searches/41316943
  - **Federal Financial Institutions Examination Council, "FFIEC Encourages Standardized Approach to Assessing Cybersecurity Preparedness," Aug. 28, 2019.** Recommends the Critical Security Controls as one of four specific tools. The FFIEC prescribes uniform principles, standards, and report forms and to promote uniformity in the supervision of financial institutions. https://www.ffiec.gov/press/pr082819.htm
  - **Conference of State Bank Supervisors, "Cybersecurity 101, A Resource Guide for Bank Executives," 2017.** Recommends use of the Critical Security Controls at 8, 12, 24. https://www.csbs.org/sites/default/files/cybersecurity101_2019_final_with_links.pdf
  - **FCC Notice of Proposed Rule Making, Dec 2022-Jan 2023):** FCC proposes measures to protect the nation's critical communications systems from cyber threats by adoption the CISA Cybersecurity Baseline or the CIS Controls. FCC NPRM, No. 22-82, Appendix B, Section E, paragraph 66, page 52: https://www.fcc.gov/document/fcc-acts-strengthen-security-nations-alerting-systems
  - **FCC, Communications Security, Reliability and Interoperability Council, CSRIC IV, Working Group 3,** "Emergency Alert System (EAS) Initial Security Subcommittee Report," May 2014. Recommending CIS Controls (then known as the "SANS 20 Critical Security Controls") as

part of its recommended Network and Operational Controls. https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG-3_Initial-Report_061814.pdf

- **FCC, Communications Security, Reliability and Interoperability Council, CISRIC III, Working Group 11, "Consensus Cyber Security Controls Final Report," March 2013.** This report finds that the "user community within Working Group 11 would prefer for the FCC to encourage industry to use the 20 Controls because they believe that the 20 Controls will protect the network infrastructure directly. The user group also believes that the 20 Controls have been demonstrated to be effective in protecting critical infrastructure from attacks that are likely to come through the enterprise systems and therefore the 20 Controls should be used by the communications industry." Report at page 8. https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG11_Report_March_%202013Final.pdf
- **NIST, U.S. Resilience Project, "Best Practices in Cyber Supply Chain Risk Management."** Boeing's IS team stated that its "primary standard is the Critical Security Controls." See at 4. https://www.nist.gov/system/files/documents/itl/csd/NIST_USRP-Boeing-Exostar-Case-Study.pdf
- **U.S. Department of Transportation, Federal Highway Administration, Transportation Management Center Information Technology Security, Final Report,** Sep. 2019. Critical Security Controls cited throughout as insight into basic practices that serve as a starting point or baseline for organizations with limited resources and cybersecurity expertise, as well as guidelines for Traffic Management Centers looking to increase their system maturity. https://ops.fhwa.dot.gov/publications/fhwahop19059/fhwahop19059.pdf
- **State of California, "California Data Breach Report," Feb. 2016.** Attorney General Kamala Harris' report warns that failing to implement all relevant Controls in California "constitutes a lack of reasonable security." The Report effectively constituted a ground-breaking minimum level of information security. See https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf . Subsequent analysis cites the endorsement of the Controls as reasonable security: https://www.littler.com/publication-press/publication/employers-receive-last-minute-reprieve-most-onerous-ccpa-compliance?utm_source=Mondaq&utm_medium=syndication&utm_campaign=View-Original
- **State of Colorado, Data Security Best Practices.** The Colorado Attorney General Data Security Best Practices guide states that: "While each entity's data security needs and practices may differ, there are some common best practices that most, if not all covered entities can implement." The guide recommends the CIS Critical Security Controls as part of Step 2, the written information security policy at 3. https://coag.gov/app/uploads/2022/01/Data-Security-Best-Practices.pdf
- **World Economic Forum (WEF), White Paper, Global Agenda Council on Cybersecurity, World Economic Forum, Apr. 2016.** Listed CIS Controls as the first best practice at 19, CIS cyber hygiene at Appendix A at page 26. http://www3.weforum.org/docs/GAC16_Cybersecurity_WhitePaper_.pdf

- **ENISA (European Union Agency for Network and Information Security), "Technical Guidelines for the implementation of minimum security measures for Digital Service Providers," Dec. 2016.** This document cited the CIS Controls as a means for meeting EU Directive 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS). See page 10 and mapping throughout. https://www.enisa.europa.eu/publications/minimum-security-measures-for-digital-service-providers/at_download/fullReport
- **ETSI (European Telecommunications Standards Institute).** The ETSI transposed all of the CIS Critical Security Controls and Safeguards and associated facilitation mechanisms into formal international specifications for global citation and normative use within the European Union. The CIS Controls were also designated as the means of implementing most of the provisions of the of the original and recently adopted European Union (EU) Revised Network and Information Security (NIS2).
  - ETSI TR 103 305-1: "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls," https://www.etsi.org/deliver/etsi_tr/103300_103399/10330501/04.01.02_60/tr_10330501v040102p.pdf
  - ETSI TR 103 305-3: "CYBER; Critical Security Controls for Effective Cyber Defence; Part 3: Service Sector Implementations," https://www.etsi.org/deliver/etsi_tr/103300_103399/10330503/02.01.01_60/tr_10330503v020101p.pdf
  - ETSI TR 103 305-4: "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Part 4: Facilitation Mechanisms," https://www.etsi.org/deliver/etsi_tr/103300_103399/10330504/02.01.01_60/tr_10330504v020101p.pdf
  - ETSI TR 103 305-5: "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Part 5: Part 5: Privacy and personal data protection enhancement," https://www.etsi.org/deliver/etsi_tr/103300_103399/10330505/02.01.01_60/tr_10330505v020101p.pdf
  - ETSI TR 103 456: "CYBER; Implementation of the Network and Information Security (NIS) Directive," https://www.etsi.org/deliver/etsi_tr/103400_103499/103456/01.01.01_60/tr_103456v010101p.pdf
  - ETSI TR 103 866: "Cyber Security (CYBER); Implementation of the Revised Network and Information Security (NIS2) Directive applying Critical Security Controls," https://www.etsi.org/deliver/etsi_tr/103800_103899/103866/01.01.01_60/tr_103866v010101p.pdf

APPENDIX E

Case History: A U.S.-Based Light Manufacturer

Identity of business withheld

Efficiency, service, and smart risk management are paramount in the light manufacturing arena. Modern practices require integration of customer data, including designs, product specs, and client identifiers. Robust information governance is critical to security and good customer service.

This case history highlights a real, light manufacturing business in the United States, the data security challenges it was facing, and its adoption of the CIS Controls as an ongoing solution.

Business Overview (Anonyco, Inc.)

To preserve security and confidentiality, the company will be referenced in this document as Anonyco, a pseudonym. Anonyco is a business-to-business operation located in the American Southwest, in a city with a population of more than one million. Its clients are business-to-consumer entities in a broad assortment of categories.

At any given time, Anonyco will have between 10-20 employees. Three are in managerial roles, including the owner and company president. The balance are in production. At least one employee works from home. There is a receptionist who interfaces with clients and delivery personnel.

It should be noted that the company president is a sophisticated business manager, and is not a technology neophyte, having at least some background in coding and software design. This detail is meaningful because experience tells us there is often no correlation between business competence and sound information governance.

Over a two-to-three-year period, Anonyco experienced a series of events stemming from apparent unauthorized access. In one very costly event, a former employee with access to client data took a job with Anonyco's competitor, poaching a client with a long-term potential value of seven figures.

Using knowledge about Anonyco and its internal operations, the former employee gained remote access to a system on Anonyco's premises. Pretending to be still employed by Anonyco, the former employee interacted with customers. The seven-figure contract was negotiated (seemingly on behalf of Anonyco) and given a, green light but at the last moment the business was referred to the competitor where the employee now worked. This incident is an ingenious example of malicious unauthorized access, but further details are withheld here, for the security of the business.

After receiving a tip, Anonyco's president reviewed event logs and confirmed repeated unauthorized access to the system. Still simmering from this blow, he continued to be concerned about data exposure, business interruptions, and revenue loss. The turning point came as Anonyco's stature grew, and it began negotiating for business from several heavily-regulated industries with oversight from

state and/or federal agencies. Client compliance requirements included data security mandates. This prompted worries about liability, and an acknowledgment from Anonyco that data security slip-ups could lead to costly litigation.

Information Governance Risks in Light Manufacturing

In the interconnected world of modern manufacturing, there is a convergence of operational technologies, artificial intelligence, internet of things, and an array of other information technologies. The risk from poor information governance looms large. Poor information governance can lead to interruptions in production, and serious delays in customer deliveries. Base-level risks exist concerning sensitive client and employee data, and the company's financial transactions. Legal jeopardy is a consequence of poor information management that's often overlooked. Small businesses rarely contemplate the role of stored information—especially digital information—in legal defense. Poor information management greatly complicates eDiscovery—reducing the chance of a solid defense—and driving up time and costs for legal representation.

Anonyco's Introduction to the CIS Controls

Anonyco's decision to adopt the CIS Controls stemmed from the desire to establish a comprehensive information governance and cybersecurity framework. After discussion, Anonyco's management understood that the CIS Controls provide a practical and prioritized approach to fortifying defenses, managing vulnerabilities, responding effectively to cyber incidents, and reducing the costs associated with litigation and regulatory compliance.

Anonyco's CIS implementation began with risk assessment, which uncovered significant vulnerabilities, as follows:

- Network misconfigurations
- Inadequate HR processes, including onboarding and off-boarding, and security training
- Unauthorized remote access
- Inadequate authentication policies
- Poor email security

Over a series of months, Anonyco proceeded as follows. All measures taken increase security and proactively boost an effective defense in case of litigation:

1 **Inventory and Control of Hardware Information Assets.** The company started by meticulously cataloging and monitoring all hardware information assets connected to the network. This step provides visibility into infrastructure, reducing the risk of unauthorized devices compromising data and other systems.

2 **Secure Configuration for Hardware and Software.** By adhering to secure configuration principles outlined by CIS, all hardware and software components have been configured for security. This mitigates the risk of cyber exploits due to misconfiguration.

3 **Controlled Use of Administrative Privileges.** Restricting access to sensitive systems and information through controlled administrative privileges has been a priority. This principle helps prevent unauthorized access and reduces the likelihood of insider threats.

4 **Data Protection.** CIS Controls guide efforts in implementing robust data protection measures. Encryption, access controls, and regular data backups are employed to safeguard critical information against unauthorized access, potential data loss, and the loss of data integrity.

5 **Continuous Vulnerability Assessment.** Regular vulnerability assessments are being conducted to identify and address potential weaknesses. This proactive approach helps to anticipate cyber threats, minimizing the risk of exploitation. Identifying vulnerabilities also helps protect data integrity: The ability to rely upon the accuracy of the business's data.

6 **Email and Web Browser Protections.** CIS-compliant email and web browser protections reduce the risk that employees will fall victim to malicious links or malicious attachments. The protection process includes user training and strong filtering mechanisms.

7 **Email and internet activities are frequently tapped for evidence during litigation.** These measures help ensure email integrity when litigation occurs.

8 **Boundary Defense.** A robust boundary defense strategy monitors and control incoming and outgoing network traffic. CIS Controls advocate for the establishment and monitoring of network perimeters to safeguard incoming and outgoing traffic, preventing unauthorized access and potential threats.

9 **Incident Response and Management.** Anonyco has developed an incident response plan that's aligned with CIS Controls. The plan includes procedures for detecting, responding to, and recovering from cybersecurity incidents.

10 **Data Recovery Capabilities.** Anonyco now regularly tests its data recovery capabilities, according to CIS recommendations, to ensure that operations can resume promptly with minimal disruption.

11 **Information Security Training.** Anonyco has and will continue to conduct training. The CIS Controls emphasize educating people on the ways they become human firewalls against risks. This includes training staff to use their cognitive skills to recognize and mitigate risks, practice secure behaviors, and fosters a culture of vigilance and risk reduction.

It should be noted that Anonyco's staff was enthusiastic about the initial training, which was conducted during an Anonyco-hosted lunch. Staff asked a lot of good questions and were pleased to have an unambiguous path to follow.

Conclusion

By proactively governing data, addressing potential vulnerabilities, and being aware of legal and regulatory liabilities, Anonyco is better positioned to grow by serving its customers. The strategic implementation of the CIS Controls has fortified the company's cybersecurity defenses and instilled a culture of vigilance and risk reduction.

APPENDIX F

Framework Mapping

The CIS Controls are mapped to many existing frameworks. Many organizations must report progress against multiple security frameworks or sets of requirements. CIS develops freely available, industry-vetted mappings to and from CIS products to all major security frameworks, including:

- Australian Signals Directorate "Essential Eight"
- CISA's Cross-Sector Cybersecurity Performance Goals (CPGs)
- CMMC v2.0
- Criminal Justice Information Services (CJIS)
- Cloud Security Alliance (CSA) Cloud Control Matrix
- Cyber Risk Institute (CRI) Profile
- FFIEC CAT
- GSMA FS.31 Baseline Security Controls
- HIPAA
- ISACA COBIT 19
- ISO 27001:2022
- ISO/IEC 27002:2022
- Microsoft Security Benchmark
- MITRE ATT&CK v8.2:
- NERC-CIP
- New Zealand Information Security Manual
- NIST CSF 1.0
- NIST CSF 2.0
- NIST 800-53 Rev. 5
- NIST SP 800-171 Rev 2
- NYS Department of Financial Services 23 NYCRR Part 500
- PCI DSS
- SOC 2
- TSA Security Directive Pipeline
- UK Cyber Essentials v2.2
- UK NCSC Cyber Assessment Framework v3.1

Details for the full list can be seen at this link under the tab titled "Mappings": https://www.cisecurity.org/controls/cis-controls-navigator/

APPENDIX G

CIS Critical Security Controls Grouped as Common-Sense Components

The CIS Critical Security Controls that are further expanded upon in Appendix H can be summarized in logical groups: know your environment; account and configuration management; security tools; data recovery; security awareness; and business processes and outsourcing.

Organizations should know their environment. Specifically, they should:

- Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure, physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate.
- Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.
- Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.

Organizations should also perform account and configuration management. Specifically, they should:

- Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications).
- Use processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts, as well as service accounts, to enterprise assets and software.
- Use processes and tools to create, assign, manage, and revoke access credentials and privileges for user, administrator, and service accounts for enterprise assets and software.
- Develop a plan to continuously assess and track vulnerabilities on all enterprise assets within the enterprise's infrastructure, in order to remediate, and minimize, the window of opportunity for attackers. Monitor public and private industry sources for new threat and vulnerability information.
- Collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack.

- Establish, implement, and actively manage (track, report, correct) network devices, in order to prevent attackers from exploiting vulnerable network services and access points.
- Manage the security life cycle of in-house developed, hosted, or acquired software to prevent, detect, and remediate security weaknesses before they can impact the enterprise.
- Commercial security tools may be used to protect against common attacks, such as specific intrusions or malware.
- Improve protections and detections of threats from email and web vectors, as these are opportunities for attackers to manipulate human behavior through direct engagement.
- Prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets.
- Operate processes and tooling to establish and maintain comprehensive network monitoring and defense against security threats across the enterprise's network infrastructure and user base.

Organizations should put in place a data recovery plan to respond and recover from an incident. Specifically, they should:

- Establish and maintain data recovery practices sufficient to restore in-scope enterprise assets to a pre-incident and trusted state.
- Establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack.
- Organizations should put in place a security awareness program. Specifically, they should:
- Establish and maintain a security awareness program to influence behavior among the workforce to be security conscious and properly skilled to reduce cybersecurity risks to the enterprise.
- Test the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in controls (people, processes, and technology), and simulating the objectives and actions of an attacker.

Organizations must put in place processes to evaluate and monitor service providers. Specifically, they should:

- Develop a process to evaluate service providers who hold sensitive data, or are responsible for an enterprise's critical IT platforms or processes, to ensure these providers are protecting those platforms and data appropriately.

APPENDIX H

Implementing All 153 Safeguards of the CIS Critical Security Controls

The following provides a full implementation of the CIS Critical Security Controls, and the underlying actions that support the Controls, i.e., a description of prescriptive and prioritized activities that organizations should take to defend their enterprise.

The priority described below was derived through a community consensus process leveraging cybersecurity experts from academia, government, and corporate entities.

In priority order, organizations should implement each of the 18 CIS Controls, starting with CIS Control 1:

1. Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure, physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate.
2. Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.
3. Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.
4. Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications).
5. Use processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts, as well as service accounts, to enterprise assets and software.
6. Use processes and tools to create, assign, manage, and revoke access credentials and privileges for user, administrator, and service accounts for enterprise assets and software.

7 Develop a plan to continuously assess and track vulnerabilities on all enterprise assets within the enterprise's infrastructure, in order to remediate, and minimize, the window of opportunity for attackers. Monitor public and private industry sources for new threat and vulnerability information.

8 Collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack.

9 Improve protections and detections of threats from email and web vectors, as these are opportunities for attackers to manipulate human behavior through direct engagement.

10 Prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets.

11 Establish and maintain data recovery practices sufficient to restore in-scope enterprise assets to a pre-incident and trusted state.

12 Establish, implement, and actively manage (i.e., track, report, and correct) network devices, in order to prevent attackers from exploiting vulnerable network services and access points.

13 Operate processes and tooling to establish and maintain comprehensive network monitoring and defense against security threats across the enterprise's network infrastructure and user base.

14 Establish and maintain a security awareness program to influence behavior among the workforce to be security conscious and properly skilled to reduce cybersecurity risks to the enterprise.

15 Develop a process to evaluate service providers who hold sensitive data, or are responsible for an enterprise's critical IT platforms or processes, to ensure these providers are protecting those platforms and data appropriately.

16 Manage the security life cycle of in-house developed, hosted, or acquired software to prevent, detect, and remediate security weaknesses before they can impact the enterprise.

17 Establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack.

18 Test the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in controls (e.g., people, processes, and technology), and simulating the objectives and actions of an attacker.

Control 1: Inventory and Control of Enterprise Assets

Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure, physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate.

1.1 Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. For mobile end-user devices, MDM type tools can support this process, where appropriate. This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. Additionally, it includes assets that are regularly connected to the enterprise's network infrastructure, even if they are not under control of the enterprise. Steps include:

- Ensure the inventory records the network address (if static), hardware address, machine name, data asset owner, department for each asset, and whether the asset has been approved to connect to the network.
- Review and update the inventory of all enterprise assets bi-annually, or more frequently.

1.2 Ensure that a process exists to address unauthorized assets on a weekly basis. The enterprise may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset. Steps include:

- After creating a list of approved assets, detect devices that are unauthorized.
- Check to see if the unauthorized asset should be authorized and update the asset inventory form.
- Otherwise, the policy to: remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.
- Address unauthorized assets on a weekly basis.

1.3 Utilize an active discovery tool to identify assets connected to the enterprise's network. Configure the active discovery tool to execute daily, or more frequently. Steps include:

- Create a list of enterprise active discovery tools.
- Run, at least daily, your active discovery tool(s).
- Add authorized assets to the approved asset inventory list and update as appropriate.

1.4 Use DHCP logging on all DHCP servers or Internet Protocol (IP) address management tools to update the enterprise's asset inventory. Review and use logs to update the enterprise's asset inventory weekly, or more frequently. Steps include:

- Use the enterprise asset inventory to create a list of DHCP and CMDB servers.
- For each DHCP server, ensure DHCP logging is enabled.
- For each CMDB server, ensure DHCP logs are used to update IP addresses.
- Add authorized assets to the approved asset inventory list and update as appropriate.

1.5 Use a passive discovery tool to identify assets connected to the enterprise's network. Review and use scans to update the enterprise's asset inventory at least weekly, or more frequently. Steps include:

- Create a list of passive asset discovery tools in use by the organization. For each, include the location of the tool's configuration information and which networks it covers.
- For each passive asset discovery tool, ensure that it is configured properly.
- Ensure that every network in the enterprise is covered by a passive asset discovery tool.
- Add authorized assets to the approved asset inventory list and update as appropriate

Control 2: Inventory and Control of Software Assets

Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

2.1 Establish and maintain a detailed inventory of all licensed software installed on enterprise assets. Steps include:

- Ensure software inventory documents the title, publisher, initial install/use date, and business purpose for each entry; where appropriate, include the Uniform Resource Locator (URL), app store(s), version(s), deployment mechanism, and decommission date.
- Review and update the software inventory bi-annually, or more frequently.

2.2 Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently. Steps include:

- Use the software asset inventory and determine if the software is "supported" or "unsupported".
- If software is "unsupported" then either document an exception or designate as unauthorized and remove, depending upon policy.

2.3 Address unauthorized software. Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently. Steps include:

- Using the enterprise asset and authorized software inventories, the enterprise must define a timeframe for scanning enterprise assets for software.
- Any software discovered that is not on the authorized software inventory must be addressed according to policy.
- If necessary, update the software inventory.
- This must be done monthly or more frequently.

2.4 Utilize automated software inventory tools, when possible, throughout the enterprise to automate the discovery and documentation of installed software. Steps include:

- Use the enterprise asset inventory to identify and enumerate assets capable of running automated software inventory tools.
- If an asset cannot support a software inventory tool, this must be documented.

2.5 Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently. Steps include:

- Identify and enumerate assets capable of supporting allowlisting software (some assets may not enable third-party software installation or otherwise have constrained environments precluding the use of allowlisting software).
- Identify all authorized allowlisting software within the enterprise.
- Identify and document allowlisting software configurations.
- Ensure allowlisting software is properly configured.

- Document assets without allowlisting software.
- Reassess bi-annually or more frequently.

2.6 Use technical controls to ensure that only authorized software libraries, such as specific .dll, .ocx, .so, etc. files, are allowed to load into a system process. Block unauthorized libraries from loading into a system process. Reassess bi-annually, or more frequently. Steps include:

- Create a list of authorized software libraries.
- Identify and enumerate allowlisting software properly configured to allow process loading of authorized libraries.
- Identify and enumerate allowlisting software improperly configured to allow process loading of authorized libraries.
- Update configurations as appropriate.
- Reassess bi-annually, or more frequently.

2.7 Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc. files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently. Steps include:

- Create a list of authorized scripts.
- Identify and enumerate all enterprise authorized software capable of executing scripts, including allowlisting software, email client applications, and web client applications
- Identify approved configurations for all software identified in above step.
- Ensure that software is properly configured to allow execution of authorized and signed scripts.
- Update configurations as appropriate.
- Reassess bi-annually, or more frequently.

Control 3: Data Protection

Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.

3.1 Establish and maintain a data management process. Steps include:

- Create a process to address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise.
- Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

3.2 Establish and maintain a data inventory based on the enterprise's data management process. Inventory sensitive data, at a minimum. Review and update inventory annually, at a minimum, with a priority on sensitive data. Steps include:

- Enumerate and identify sensitive data.
- Map the sensitive data to the organizations data scheme and the enterprise asset it is located on.
- Review and update inventory annually, at a minimum, with a priority on sensitive data.

3.3 Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. Steps include:

- Use the documented data management process, as guidelines to map which user accounts have access to sensitive data.
- For each enterprise asset that stores sensitive data, apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.

3.4 Retain data according to the enterprise's data management process. Data retention must include both minimum and maximum timelines.

- Identify and enumerate sensitive data types with defined minimum and maximum retention rates.
- Identify and enumerate items in the inventory that comply with retention timelines.
- Identify and enumerate items in the inventory that do not comply with retention timeline.
- Take steps to come into data retention compliance.

3.5 Securely dispose of data as outlined in the enterprise's data management process. Ensure the disposal process and method are commensurate with the data sensitivity. Steps include:

- Identify and enumerate each sensitive data type with a disposal method and process as defined by the data management process.
- Ensure all sensitive data complies with disposal requirements.

3.6 Encrypt data on end-user devices containing sensitive data. Example implementations can include Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.

- Use the enterprise asset inventory to identify and enumerate end-user devices with sensitive data.
- identify and enumerate the end-user devices that have encryption software installed.
- Identify and enumerate the end-user devices without encryption software. Document exceptions as necessary. Otherwise, bring end-user devices into compliance with data policy.
- For end-user devices that have encryption software, ensure that the encryption software is properly configured.

3.7 Establish and maintain an overall data classification scheme for the enterprise. Enterprises may use labels, such as "Sensitive", "Confidential" and "Public", and classify their data according to those labels. Steps include:

- Create a data classification and apply it to the sensitive data types.
- Review and update the classification scheme annually, or when significant enterprise changes occur that could impact this Safeguard.

3.8 Document data flows. Data flow documentation includes service provider data flows and should be based on the enterprise's data management process. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. Steps include:

- Create documentation outlining data flow for enterprise-owned data. Documentation should include, at a minimum, data flows to external enterprises.
- Review and update the classification scheme annually, or when significant enterprise changes occur that could impact this Safeguard.

3.9 Encrypt data on removable media. Steps include:

- Use the enterprise asset inventory to identify and enumerate assets authorized to support removable media.
- Use the authorized software inventory to identify encryption software identified on the above assets.
- Identify and enumerate the assets without encryption software installed.
- Install encryption software where possible on the assets identified above. Document exceptions.
- Ensure all identified assets have properly configured encryption software.

3.10 Encrypt sensitive data in transit. Example implementations can include Transport Layer Security (TLS) and Open Secure Shell (OpenSSH). Steps include:

- Using the sensitive data inventory, identify the means and components for encrypting data in transit.
- Ensure the software is configured properly and enable the encryption chosen.

3.11 Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data. Steps include:

- Use the authorized software asset inventory to identify and enumerate all encryption tools requiring secondary authentication systems.
- Use the enterprise asset inventory and the sensitive data inventory to identify and enumerate all enterprise assets storing sensitive data.
- Ensure all assets with sensitive data are configured properly to encrypt data at rest.

3.12 Organizations must segment data processing and storage based on the sensitivity of the data. Do not process sensitive data on enterprise assets intended for lower sensitivity data. An asset's overall sensitivity level should be the highest sensitivity level of the data it stores/processes/transmits. If a system contains any sensitive information, that asset should be treated accordingly and should be properly separated from networks or network segments that do not need to access that type of sensitive information. Steps include:

- Use the sensitive data inventory to identify the assets that store, process, or transmit sensitive data.
- Using the data from the above step, identify all networks/VLANS connected to the assets that store, process, or transmit sensitive data.

- Identify and enumerate any instances of properly separated assets from less sensitive networks.
- Identify and enumerate any instances of improperly separated assets from less sensitive networks.
- Take steps to ensure proper separation of sensitive data on assets.

3.13 Implement an automated tool, such as a host-based Data Loss Prevention (DLP) tool to identify all sensitive data stored, processed, or transmitted through enterprise assets, including those located onsite or at a remote service provider, and update the enterprise's sensitive data inventory. Steps include:

- Use the authorized software inventory to identify and enumerate all data loss prevention software.
- Ensure that each enterprise asset that stores, processes, or transmits sensitive data has data loss prevention software installed.
- Ensure that the data loss prevention software is properly configured.

3.14 Log sensitive data access, including modification and disposal. Steps include:

- Use the authorized software inventory to identify authorized logging software.
- Ensure that enterprise assets that store, process, or transmit sensitive data has logging software installed.
- Ensure that the logging software is properly configured.

Control 4: Secure Configuration of Enterprise Assets and Software

Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications).

4.1 Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Steps include:

- Use the enterprise asset inventory to identify and enumerate end-user devices, including portable and mobile, non-computing/IoT devices, and servers.
- Use the authorized software asset inventory to identify and enumerate the software installed on assets.

- Check if there is a configuration standard that can be applied to installed software. A configuration standard may include industry standard baselines such as CIS benchmarks, DISA Security Technical Implementation Guides (STIGs), or U.S. government configuration baselines (USGCB).
- Apply configuration standards where appropriate.
- Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

4.2 Establish and maintain a secure configuration process for network devices. Steps include:

- Use the enterprise asset inventory to identify and enumerate network infrastructure assets.
- Use the authorized software asset inventory to identify and enumerate the software installed on those network infrastructure assets.
- Check if there is a configuration standard that can be applied to installed software. A configuration standard may include industry standard baselines such as CIS benchmarks, DISA Security Technical Implementation Guides (STIGs), or U.S. government configuration baselines (USGCB).
- Apply configuration standards where appropriate.
- Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

4.3 Configure automatic session locking on enterprise assets after a defined period of inactivity. For general-purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes. Steps include:

- Identify and enumerate assets that support automatic locking due to inactivity.
- For general computing assets, ensure properly configured automatic locking (15 minutes or less).
- For mobile assets, ensure properly configured automatic locking (2 minutes or less).

4.4 Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, an operating system firewall, or a third-party firewall agent. Steps include:

- Identify and enumerate servers capable of hosting a firewall.
- Identify and enumerate applications capable of hosting a firewall.
- Ensure that firewalls are properly configured using configuration standards.

4.5 Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed. Steps include:

- Identify and enumerate end-user devices capable of hosting a firewall or a deny rule.
- Use configuration standards to ensure firewalls or deny rules are properly configured on end-user devices.

4.6 Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential. Steps include:

- Identify and enumerate assets with authorized management software installed.
- Use configuration standards to ensure that management software is configured properly.

4.7 Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include disabling default accounts or making them unusable. Steps include:

- Identify and enumerate authorized operating software, applications, and third-party software that contain default accounts on enterprise assets.
- Enumerate default accounts.
- Check if default accounts can be disabled and disable if possible.
- If an account cannot be disabled, ensure to change default passwords according to the enterprise's unique password policy.
- Document default accounts with changed passwords.

4.8 Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file-sharing service, web application module, or service function. Steps include:

- Identify and enumerate authorized services.
- Identify and enumerate all services on enterprise assets.
- Identify and enumerate authorized services on assets.
- Identify and enumerate unauthorized services on assets.
- Take care of unauthorized services on assets according to policy.
- Check configurations on authorized services to make sure they are configured properly.

4.9 Configure trusted DNS servers on enterprise assets. Example implementations include configuring assets to use enterprise-controlled DNS servers and/or reputable externally accessible DNS servers. Steps include:

- Identify and enumerate authorized DNS servers.
- Identify and enumerate assets configured for authorized DNS servers.
- Check the configuration of DNS servers identified on assets to ensure they are configured with the authorized DNS servers.

4.10 Enforce automatic device lockout following a predetermined threshold of local failed authentication attempts on portable end-user devices, where supported. For laptops, do not allow more than 20 failed authentication attempts; for tablets and smartphones, no more than 10 failed authentication attempts. Example implementations include Microsoft InTune Device Lock and Apple Configuration Profile maxFailedAttempts. Steps include:

- Identify and enumerate all portable devices.
- Check failed authentication configuration for all portable devices.
  - Ensure that failed authentication on laptops is properly configured to 20 failed attempts or less.
  - Ensure that failed authentication on mobile devices is properly configured to 10 failed attempts or less.

4.11 Remotely wipe enterprise data from enterprise-owned portable end-user devices when deemed appropriate such as lost or stolen devices, or when an individual no longer supports the enterprise. Steps include:

- Identify and enumerate portable end-user devices that support remote wipe.
- Ensure proper configuration for remote wipe on portable devices capable of supporting remote wipe.

4.12 Ensure separate enterprise workspaces are used on mobile end-user devices, where supported. Example implementations include using an Apple Configuration Profile or Android Work Profile to separate enterprise applications and data from personal applications and data. Steps include:

- Identify and enumerate authorized mobile device management software.
- Identify mobile devices capable of supporting mobile device management software.
- Ensure proper configurations of mobile devices with mobile device management software.

Control 5: Account Management

Use processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts, as well as service accounts, to enterprise assets and software.

5.1 Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Steps include:

- Create an inventory of accounts and document the following elements: person's name, username, start/stop dates, and department.
- Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.
- Validate that all inactive accounts are disabled/removed, on a recurring schedule at a minimum quarterly, or more frequently.

5.2 Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.

5.3 Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.

5.4 Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.

5.5 Establish and maintain an inventory of service accounts. The inventory, at a minimum, must contain the department owner, review date, and purpose. Steps include:

- Using the inventory of accounts, ensure that the following elements are present: department owner, review date, and purpose.
- Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.

5.6 Centralize account management through a directory or identity service. Steps include:

- Identify and enumerate centralized authentication points.
- For each centralized authentication point identified, determine whether it is necessary or can be consolidated.
- Where appropriate, consolidate centralized authentication points.

Control 6: Access Control Management

Use processes and tools to create, assign, manage, and revoke access credentials and privileges for user, administrator, and service accounts for enterprise assets and software.

6.1 Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.

6.2 Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.

6.3 Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard. Steps include:

- Identify and enumerate externally exposed and third-party applications.
- Identify and enumerate all user accounts associated with the applications.
- Ensure the user accounts are properly configured to use MFA.

6.4 Require MFA for remote network access. Steps include:

- Identify and enumerate all authorized remote assets.
- Ensure that all authorized remote assets are properly configured to require MFA.

6.5 Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider. Steps include:

- Identify and enumerate all administrative accounts.
- Ensure that all administrative accounts are properly configured to require MFA.

6.6 Establish and maintain an inventory of the enterprise's authentication and authorization systems, including those hosted on-site or at a remote service provider. Review and update the inventory, at a minimum, annually, or more frequently.

6.7 Centralize access control for all enterprise assets through a directory service or SSO provider, where supported. Steps include:

- Identify all directory and SSO services.
- Identify and enumerate assets that support directory and SSO services.
- Ensure each asset is covered by at least one directory or SSO service.

6.8 Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.

Control 7: Continuous Vulnerability Management

Develop a plan to continuously assess and track vulnerabilities on all enterprise assets within the enterprise's infrastructure, in order to remediate, and minimize, the window of opportunity for attackers. Monitor public and private industry sources for new threat and vulnerability information.

7.1 Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

7.2 Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.

7.3 Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis. Steps include:

- Identify authorized operating systems within the enterprise.
- Identify the operating system currently running on each asset.
- For each asset:
  - Identify and enumerate operating systems that are up to date.
  - Identify and enumerate operating systems that are not up to date.
- For each out-of-date operating system identified, determine whether there is a documented exception. Take corrective action as appropriate.
- Identify authorized automated patch management software.
- Identify and enumerate operating systems covered by at least one automated patch management software.
- Identify and enumerate operating systems not covered by at least one automated patch management software. Take corrective action as appropriate.
- Ensure that the automated patch management software is configured to run every 30 days or less.

7.4 Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis. Steps include:

- Identify authorized applications within the enterprise.
- Identify the applications currently running on each asset.
- For each asset:
  - Identify and enumerate applications that are up to date.
  - Identify and enumerate applications that are not up to date.
- For each out-of-date application identified, determine whether there is a documented exception. Take corrective action as appropriate.
- Identify and enumerate applications covered by at least one automated patch management software.
- Identify and enumerate operating systems not covered by at least one automated patch management software. Take corrective action as appropriate.
- Ensure that the automated patch management software is configured to run every 30 days or less.

7.5 Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool. Steps include:

- Identify and enumerate vulnerability scanning software.
- Identify and enumerate authenticated vulnerability scanning software.
- Use enterprise asset inventory to identify and enumerate all internal assets.
- Identify and enumerate internal assets covered by at least one vulnerability scanning software.
- Identify and enumerate internal assets not covered by at least one vulnerability scanning software. Take corrective action as appropriate.
- Ensure vulnerability scanning software is configured to scan every 3 months or less.
- Identify and enumerate internal assets covered by at least one authenticated vulnerability scanner.
- Identify and enumerate internal assets not covered by at least one authenticated vulnerability scanner. Take corrective action as appropriate.
- Ensure authenticated vulnerability scanning software is configured to scan every 3 months or less.

7.6 Perform automated vulnerability scans of externally exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis. Steps include:

- Use the enterprise asset inventory to identify and enumerate all external assets.
- Identify and enumerate external assets covered by at least one vulnerability scanning software.
- Identify and enumerate external assets not covered by at least one vulnerability scanning software. Take corrective action as appropriate.
- Ensure that vulnerability scanners are properly configured to scan every 30 days or less.

7.7 Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.

Control 8: Audit Log Management

Collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack.

8.1 Establish and maintain an audit log management process that defines the enterprise's logging requirements. At a minimum, address the collection, review, and retention of audit logs for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

8.2 Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets. Steps include:

- Use the enterprise asset inventory to identify and enumerate assets capable of supporting logging.
- Ensure that assets are properly configured to log events per the process.

8.3 Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.

8.4 Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported. Steps include:

- Identify and enumerate assets capable of supporting time synchronization.
- Ensure that the assets are configured using at least two approved time sources.

8.5 Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.

8.6 Collect DNS query audit logs on enterprise assets, where appropriate and supported. Steps include:

- Identify and enumerate internal DNS Servers.
- Ensure that the DNS servers are properly configured to collect logs.

8.7 Collect URL request audit logs on enterprise assets, where appropriate and supported. Steps include:

- Identify and enumerate assets that support URL logging.
- Ensure that the assets are properly configured for logging.

8.8 Collect command-line audit logs. Example implementations include collecting audit logs from PowerShell®, BASH™, and remote administrative terminals. Steps include:

- Use the asset inventory to identify and enumerate assets that support command-line auditing of command.
- Ensure that the assets are properly configured.

8.9 Centralize, to the extent possible, audit log collection and retention across enterprise assets. Steps include:

- Use the software inventory to identify and enumerate log aggregating software.
- Ensure that assets are covered by at least one aggregating software.

8.10 Retain audit logs across enterprise assets for a minimum of 90 days.

- Ensure aggregating software is configured to retain logs for 90 days or more.

8.11 Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. Conduct reviews on a weekly, or more frequent, basis.

8.12 Collect service provider logs, where supported. Example implementations include collecting authentication and authorization events, data creation and disposal events, and user management events.

- For each service provided in the inventory of service providers, identify and enumerate service providers that support logging.

Control 9: Email and Web Browser Protections

Improve protections and detections of threats from email and web vectors, as these are opportunities for attackers to manipulate human behavior through direct engagement.

9.1 Ensure only fully supported browsers and email clients are allowed to execute in the enterprise, only using the latest version of browsers and email clients provided through the vendor. Steps include:

- Use the authorized software inventory to identify and enumerate web browser and email client software.
- Ensure that software labeled as "supported" is currently supported by the software vendor.

9.2 Use DNS filtering services on all enterprise assets to block access to known malicious domains. Steps include:

- Use the enterprise asset inventory to identify and enumerate assets that support DNS filtering.
- Use the authorized software asset inventory to identify and enumerate authorized DNS filtering services.
- Ensure that the software is assets properly configured.

9.3 Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets. Steps include:

- Use the enterprise asset inventory to identify and enumerate enterprise assets capable of supporting network-based URL filters.
- Use the authorized software inventory to identify authorized web browsers/clients.
- Ensure that the software is properly configured.

9.4 Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications. Steps include:

- Use the enterprise asset inventory to identify and enumerate assets subject to browser/email plugin restrictions.
- Use the software asset inventory to identify authorized browser and email plugins.
- Ensure only authorized browser plugins installed or enabled.
- Ensure only authorized email plugins installed or enabled.

9.5 To lower the chance of spoofed or modified emails from valid domains, implement DMARC policy and verification, starting with implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail (DKIM) standards.

9.6 Block unnecessary file types attempting to enter the enterprise's email gateway. Steps include:

- Use the enterprise asset inventory to identify and enumerate assets configured as email gateways.
- Ensure that the email gateways properly configured to block unnecessary attachments.

9.7 Deploy and maintain email server anti-malware protections, such as attachment scanning and/or sandboxing. Steps include:

- Use the enterprise asset inventory to identify and enumerate all email servers within the enterprise.
- For each email ensure native or external anti-malware protections are configured properly.

Control 10: Malware Defense

Prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets.

10.1 Deploy and maintain anti-malware software on all enterprise assets. Steps include:

- Use the enterprise asset inventory to identify and enumerate assets capable of supporting anti-malware software.
- Use the authorized software inventory to identify authorized anti-malware software.
- Identify and enumerate assets with at least one authorized anti-malware software installed.
- Identify and enumerate assets with only unauthorized anti-malware software installed and take corrective action as appropriate.
- Identify and enumerate assets without any anti-malware software installed and take corrective action as appropriate.
- Ensure that the anti-malware software is properly configured.

10.2 Configure automatic updates for anti-malware signature files on all enterprise assets. Step includes:

- Ensure that the anti-malware software is properly configured for automatic updates.

10.3 Disable autorun and autoplay auto-execute functionality for removable media. Steps include:

- Use the enterprise asset inventory to identify and enumerate enterprise assets capable of performing autorun, autoplay, and auto-execute functions.
- Ensure that the configurations of each asset identified above disable autorun, autoplay, and auto-execute functions.

10.4 Configure anti-malware software to automatically scan removable media.

10.5 Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.

10.6 Centrally manage anti-malware software. Step includes:

- Ensure that each authorized anti-malware software is centrally managed.

10.7 Use behavior-based anti-malware software. Steps include:

- Use the enterprise asset inventory to identify and enumerate assets capable of supporting behavior-based anti-malware software.
- Use the authorized software inventory to identify authorized behavior-based anti-malware software.
- Ensure assets have at least one authorized behavior-based anti-malware software installed.
- Ensure that behavior-based anti-malware software is properly configured.

Control 11: Data Recovery

Establish and maintain data recovery practices sufficient to restore in-scope enterprise assets to a pre-incident and trusted state.

11.1 Establish and maintain a data recovery process. In the process, address the scope of data recovery activities, recovery prioritization, and the security of backup data. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

11.2 Perform automated backups of in-scope enterprise assets. Run backups weekly, or more frequently, based on the sensitivity of the data. Steps include:

- Use the enterprise asset inventory to identify and enumerate assets that are in-scope for automated backups.

- Use the authorized software inventory to identify authorized backup software and for each asset identified above.
- Ensure that assets are covered by at least one authorized backup software.
- Ensure that the backup software is configured properly.

11.3 Protect recovery data with equivalent controls to the original data. Reference encryption or data separation, based on requirements. Step includes:

- For each asset with backup software installed ensure encryption is configured for backups.

11.4 Establish and maintain an isolated instance of recovery data. Example implementations include version-controlling backup destinations through offline, cloud, or off-site systems or services. Step includes:

- Ensure that backups are properly configured to send to an isolated instance.

11.5 Test backup recovery quarterly, or more frequently, for a sampling of in-scope enterprise assets.

Control 12: Network Infrastructure Management

Establish, implement, and actively manage (track, report, correct) network devices to prevent attackers from exploiting vulnerable network services and access points.

12.1 Ensure network infrastructure is kept up-to-date. Example implementations include running the latest stable release of software and/or using currently supported network-as-a-service (NaaS) offerings. Review software versions monthly, or more frequently, to verify software support.

12.2 Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.

12.3 Securely manage network infrastructure. Example implementations include version-controlled-infrastructure-as-code, and the use of secure network protocols, such as SSH and HTTPS. Steps include:

- For network infrastructure assets, ensure they are configured to use encrypted sessions.
- For every network segment, identify and enumerate network segments that use infrastructure-as-code for the whole segment or partial.
- Ensure that network segments are covered by version-controlled infrastructure-as-code.

12.4 Establish and maintain architecture diagram(s) and/or other network system documentation. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

12.5 Centralize network Authentication, Authorization and Auditing (AAA). Steps include:

- Use the authorized software inventory to identify and enumerate all AAA services within the enterprise.
- For each centralized AAA point, determine whether it is necessary or can be consolidated.
- Ensure that each network infrastructure asset is covered by at least one AAA system.

12.6 Use secure network management and communication protocols (e.g., 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise or greater). Steps include:

- For each network segment, identify communication protocols.
- Ensure only authorized communication protocols are being used.
- Ensure the communication protocols are configured properly.
- For each network segment, identify network management protocols.
- Ensure only authorized network management protocols are being used.
- Ensure the network management protocols are configured properly.

12.7 Require users to authenticate to enterprise-managed VPN and authentication services prior to accessing enterprise resources on end-user devices. Steps include:

- Use the enterprise asset inventory to identify and enumerate remote enterprise assets.
- Use the enterprise asset inventory and software asset inventory to identify and enumerate all VPN devices and software.
- Ensure that VPN devices and software are properly configured to require authentication prior to granting access.
- Ensure appropriate assets are covered by a VPN.
- Ensure that AAA services are properly configured to require authentication prior to granting access.
- Ensure appropriate assets are covered by an AAA service.

12.8 Establish and maintain dedicated computing resources, either physically or logically separated, for all administrative tasks or tasks requiring administrative access. The computing resources should be segmented from the enterprise's primary network and not be allowed internet access. Steps include:

- Use the enterprise asset inventory to identify and enumerate assets used for administrative purposes.
- For each asset identified above, make sure they are configured to not have internet access.

Control 13: Network Monitoring and Defense

Operate processes and tooling to establish and maintain comprehensive network monitoring and defense against security threats across the enterprise's network infrastructure and user base.

13.1 Centralize security event alerting across enterprise assets for log correlation and analysis. Best practice implementation requires the use of a SIEM, which includes vendor-defined event correlation alerts. A log analytics platform configured with security-relevant correlation alerts also satisfies this Safeguard. Steps include:

- Use the enterprise asset inventory to identify and enumerate enterprise assets that produce security event logs.
- For every asset identified above ensure logs are centralized at the location of the log correlation or log analytic tool.

13.2 Deploy a host-based intrusion detection solution on enterprise assets, where appropriate and/or supported. Steps include:

- Use the enterprise asset inventory to identify and enumerate assets capable of supporting host-based intrusion detection systems.
- Use the authorized software asset inventory to identify authorized host-based intrusion detection software.
- For each asset identified above, ensure it is covered by at least one authorized host-based intrusion detection software.

13.3 Deploy a network intrusion detection solution on enterprise assets, where appropriate. Example implementations include the use of a Network Intrusion Detection System (NIDS) or equivalent cloud service provider (CSP) service. Steps include:

- Use the identified assets that are part of the network infrastructure to identify the network intrusion detection solutions for the enterprise.
- Use the Enterprise Network Architecture Documentation to identify and enumerate network boundaries.
- For each network boundary identified, ensure it is covered by at least one network intrusion detection solution.

13.4 Perform traffic filtering between network segments, where appropriate. Steps include:

- Identify and enumerate network segments that require communication with other network segments.
- For each network segment identified, identify network infrastructure assets responsible for traffic filtering, ensure each segment is properly configured to filter traffic.

13.5 Manage access control for assets remotely connecting to enterprise resources. Determine amount of access to enterprise resources based on: up-to-date anti-malware software installed, configuration compliance with the enterprise's secure configuration process, and ensuring the operating system and applications are up-to-date. Steps include:

- Use the Authentication and Authorization System Inventory to identify and enumerate authorization systems that allow remote logins.
- For each authorization system identified, ensure it is properly configured for all the policies.
- Ensure each remote asset is covered by at least one compliant authorization system.

13.6 Collect network traffic flow logs and/or network traffic to review and alert upon from network device. Steps include:

- Use assets that are part of the network infrastructure to identify and enumerate network boundary assets.
- For each network boundary asset identified ensure proper configuration to enable network traffic or network traffic flow logging,

13.7 Deploy a host-based intrusion prevention solution on enterprise assets, where appropriate and/or supported. Example implementations include use of an Endpoint Detection and Response (EDR) client or host-based IPS agent. Steps include:

- Use the enterprise asset inventory to identify and enumerate assets capable of supporting host-based intrusion prevention systems.
- Use the authorized software inventory to identify authorized host based intrusion prevention software.
- For each asset identified ensure that it is covered by at least one authorized host-based intrusion prevention software.

13.8 Deploy a network intrusion prevention solution, where appropriate. Example implementations include the use of a Network Intrusion Prevention System (NIPS) or equivalent CSP service. Steps include:

- Use assets that are part of the network infrastructure to identify the network intrusion prevention solutions for the enterprise.
- Identify network boundaries and ensure each boundary is covered by at least one network intrusion prevention solution.

13.9 Deploy port-level access control. Port-level access control utilizes 802.1x, or similar network access control protocols, such as certificates, and may incorporate user and/or device authentication. Steps include:

- Use the authorized software asset inventory to identify and enumerate 802.1x authenticators.
- For each authenticator identified, ensure it is properly configured.
- Use AAA services within the enterprise to identify 802.1x authentication servers.
- For each authentication server identified, ensure configuration includes a connection to at least one CMDB server.
- If the enterprise does not use 802.1x network design to control network access, ensure proper configuration to use client authentication certificate.

13.10 Perform application layer filtering. Example implementations include a filtering proxy, application layer firewall, or gateway. Steps include:

- Use the authorized software asset inventory to identify software used for application layer filtering.
- For assets that are part of the network infrastructure ensure that all are covered by application layer filtering software.

13.11 Tune security event alerting thresholds monthly, or more frequently.

Control 14: Security Awareness and Skills Training

Establish and maintain a security awareness program to influence behavior among the workforce to be security conscious and properly skilled to reduce cybersecurity risks to the enterprise.

14.1 Establish and maintain a security awareness program. The purpose of a security awareness program is to educate the enterprise's workforce on how to interact with enterprise assets and data in a secure manner. Conduct training at hire and, at a minimum, annually. Review and update content annually, or when significant enterprise changes occur that could impact this Safeguard.

14.2 Train workforce members to recognize social engineering attacks, such as phishing, pre-texting, and tailgating.

14.3 Train workforce members on authentication best practices. Example topics include MFA, password composition, and credential management.

14.4 Train workforce members on how to identify and properly store, transfer, archive, and destroy sensitive data. This also includes training workforce members on clear screen and desk best practices, such as locking their screen when they step away from their enterprise asset, erasing physical and virtual whiteboards at the end of meetings, and storing data and assets securely.

14.5 Train workforce members to be aware of causes for unintentional data exposure. Example topics include mis-delivery of sensitive data, losing a portable end-user device, or publishing data to unintended audiences.

14.6 Train workforce members to be able to recognize a potential incident and be able to report such an incident.

14.7 Train workforce to understand how to verify and report out-of-date software patches or any failures in automated processes and tools. Part of this training should include notifying IT personnel of any failures in automated processes and tools.

14.8 Train workforce members on the dangers of connecting to, and transmitting data over, insecure networks for enterprise activities. If the enterprise has remote workers, training must include guidance to ensure that all users securely configure their home network infrastructure.

14.9 Conduct role-specific security awareness and skills training. Example implementations include secure system administration courses for IT professionals, (OWASP® Top 10 vulnerability awareness and prevention training for web application developers, and advanced social engineering awareness training for high-profile roles.

Control 15: Service Provider Management

Develop a process to evaluate service providers who hold sensitive data, or are responsible for an enterprise's critical IT platforms or processes, to ensure these providers are protecting those platforms and data appropriately.

15.1 Establish and maintain an inventory of service providers. The inventory is to list all known service providers, include classification(s), and designate an enterprise contact for each service provider. Review and update the inventory annually, or when significant enterprise changes occur that could impact this Safeguard.

15.2 Establish and maintain a service provider management policy. Ensure the policy addresses the classification, inventory, assessment, monitoring, and decommissioning of service providers. Review and update the policy annually, or when significant enterprise changes occur that could impact this Safeguard.

15.3 Classify service providers. Classification consideration may include one or more characteristics, such as data sensitivity, data volume, availability requirements, applicable regulations, inherent risk, and mitigated risk. Update and review classifications annually, or when significant enterprise changes occur that could impact this Safeguard.

15.4 Ensure service provider contracts include security requirements. Example requirements may include minimum security program requirements, security incident and/or data breach notification and response, data encryption requirements, and data disposal commitments. These security requirements must be consistent with the enterprise's service provider management policy. Review service provider contracts annually to ensure contracts are not missing security requirements.

15.5 Assess service providers consistent with the enterprise's service provider management policy. Assessment scope may vary based on classification(s), and may include review of standardized assessment reports, such as Service Organization Control 2 (SOC 2) and Payment Card Industry (PCI) Attestation of Compliance (AoC), customized questionnaires, or other appropriately rigorous processes. Reassess service providers annually, at a minimum, or with new and renewed contracts.

15.6 Monitor service providers consistent with the enterprise's service provider management policy. Monitoring may include periodic reassessment of service provider compliance, monitoring service provider release notes, and dark web monitoring.

15.7 Securely decommission service providers. Example considerations include user and service account deactivation, termination of data flows, and secure disposal of enterprise data within service provider systems.

Control 16: Application Software Security

Manage the security life cycle of in-house developed, hosted, or acquired software to prevent, detect, and remediate security weaknesses before they can impact the enterprise.

16.1 Establish and maintain a secure application development process. In the process, address such items as: secure application design standards, secure coding practices, developer training, vulnerability management, security of third-party code, and application security testing procedures. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

16.2 Establish and maintain a process to accept and address reports of software vulnerabilities, including providing a means for external entities to report. The process is to include such items as: a vulnerability handling policy that identifies reporting process, responsible party for handling vulnerability reports, and a process for intake, assignment, remediation, and remediation testing. As part of the process, use a vulnerability tracking system that includes severity ratings, and metrics for measuring timing for identification, analysis, and remediation of vulnerabilities. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

- Third-party application developers need to consider this an externally facing policy that helps to set expectations for outside stakeholders.

16.3 Perform root cause analysis on security vulnerabilities. When reviewing vulnerabilities, root cause analysis is the task of evaluating underlying issues that create vulnerabilities in code and allows development teams to move beyond just fixing individual vulnerabilities as they arise.

16.4 Establish and manage an updated inventory of third-party components used in development, often referred to as a "bill of materials," as well as components slated for future use. This inventory is to include any risks that each third-party component could pose. Evaluate the list at least monthly to identify any changes or updates to these components and validate that the component is still supported.

16.5 Use up-to-date and trusted third-party software components. When possible, choose established and proven frameworks and libraries that provide adequate security. Acquire these components from trusted sources or evaluate the software for vulnerabilities before use.

16.6 Establish and maintain a severity rating system and process for application vulnerabilities that facilitates prioritizing the order in which discovered vulnerabilities are fixed. This process includes setting a minimum level of security acceptability for releasing code or applications. Severity ratings bring a systematic way of triaging vulnerabilities that improves risk management and helps ensure the most severe bugs are fixed first. Review and update the system and process.

16.7 Use standard, industry-recommended hardening configuration templates for application infrastructure components. This includes underlying servers, databases, and web servers, and applies to cloud containers, Platform as a Service (PaaS) components, and SaaS components. Do not allow in-house developed software to weaken configuration hardening.

16.8 Maintain separate environments for production and non-production systems.

16.9 Ensure that all software development personnel receive training in writing secure code for their specific development environment and responsibilities. Training can include general security principles and application security standard practices. Conduct training at least annually and design in a way to promote security within the development team, and build a culture of security among the developers.

16.10 Apply secure design principles in application architectures. Secure design principles include the concept of least privilege and enforcing mediation to validate every operation that the user makes, promoting the concept of "never trust user input." Examples include ensuring that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats. Secure design also means minimizing the application infrastructure attack surface, such as turning off unprotected ports and services, removing unnecessary programs and files, and renaming or removing default accounts.

16.11 Leverage vetted modules or services for application security components, such as identity management, encryption, and auditing and logging. Using platform features in critical security functions will reduce developers' workload and minimize the likelihood of design or implementation errors. Modern operating systems provide effective mechanisms for identification, authentication, and authorization and make those mechanisms available to applications. Use only standardized, currently accepted, and extensively reviewed encryption algorithms. Operating systems also provide mechanisms to create and maintain secure audit logs.

16.12 Apply static and dynamic analysis tools within the application life cycle to verify that secure coding practices are being followed.

16.13 Conduct application penetration testing. For critical applications, authenticated penetration testing is better suited to finding business logic vulnerabilities than code scanning and automated security testing. Penetration testing relies on the skill of the tester to manually manipulate an application as an authenticated and unauthenticated user.

16.14 Conduct threat modeling. Threat modeling is the process of identifying and addressing application security design flaws within a design before code is created. It is conducted through specially trained individuals who evaluate the application design and gauge security risks for each entry point and access level. The goal is to map out the application, architecture, and infrastructure in a structured way to understand its weaknesses.

Control 17: Incident Response Management

Establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack.

17.1 Designate one key person, and at least one backup, who will manage the enterprise's incident handling process. Management personnel are responsible for the coordination and documentation of incident response and recovery efforts and can consist of employees internal to the enterprise, third-party vendors, or a hybrid approach. If using a third-party vendor, designate at least one person internal to the enterprise to oversee any third-party work. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

17.2 Establish and maintain contact information for parties that need to be informed of security incidents. Contacts may include internal staff, third-party vendors, law enforcement, cyber insurance providers, relevant government agencies, Information Sharing and Analysis Center (ISAC) partners, or other stakeholders. Verify contacts annually to ensure that information is up to date.

17.3 Establish and maintain an enterprise process for the workforce to report security incidents. The process includes reporting timeframe, personnel to report to, mechanism for reporting, and the minimum information to be reported. Ensure the process is publicly available to all of the workforce. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

17.4 Establish and maintain an incident response process that addresses roles and responsibilities, compliance requirements, and a communication plan. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

17.5 Assign key roles and responsibilities for incident response, including staff from legal, IT, information security, facilities, public relations, human resources, incident responders, and analysts, as applicable. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

17.6 Determine which primary and secondary mechanisms will be used to communicate and report during a security incident. Mechanisms can include phone calls, emails, or letters. Keep in mind that certain mechanisms, such as emails, can be affected during a security incident. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

17.7 Plan and conduct routine incident response exercises and scenarios for key personnel involved in the incident response process to prepare for responding to real-world incidents. Exercises need to test communication channels, decision making, and workflows. Conduct testing on an annual basis, at a minimum.

17.8 Conduct post-incident reviews. Post-incident reviews help prevent incident recurrence through identifying lessons learned and follow-up action.

17.9 Establish and maintain security incident thresholds, including, at a minimum, differentiating between an incident and an event. Examples can include: abnormal activity, security vulnerability, security weakness, data breach, privacy incident, etc. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

Control 18: Penetration Testing

Test the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in controls (people, processes, and technology), and simulating the objectives and actions of an attacker.

18.1 Establish and maintain a penetration testing program appropriate to the size, complexity, and maturity of the enterprise. Penetration testing program characteristics include scope, such as network, web application, Application Programming Interface (API), hosted services, and physical premise controls; frequency; limitations, such as acceptable hours, and excluded attack types; point of contact information; remediation, such as how findings will be routed internally; and retrospective requirements.

18.2 Perform periodic external penetration tests based on program requirements, no less than annually. External penetration testing must include enterprise and environmental reconnaissance to detect exploitable information. Penetration testing requires specialized skills and experience and must be conducted through a qualified party. The testing may be clear box or opaque box.

18.3 Remediate penetration test findings based on the enterprise's policy for remediation scope and prioritization.

18.4 Validate security measures after each penetration test. If deemed necessary, modify rulesets and capabilities to detect the techniques used during testing.

18.5 Perform periodic internal penetration tests based on program requirements, no less than annually. The testing may be clear box or opaque box.

APPENDIX I

Methodologies to Test for Reasonable Cybersecurity

The two most obvious opportunities to apply a test for the reasonableness of cybersecurity controls are when enterprises (risk managers) are planning or evaluating the protective measures (controls and safeguards) that they implement and operate, and when a legal authority (adjudicators) must determine when controls and safeguards are reasonable. Legal authorities may be judges, juries, or arbitrators who determine liability after a security incident or may be a regulator who, during audits or investigations, evaluates the compliance of cybersecurity programs.

This appendix describes publicly available resources that model how these "ex-ante" and "ex-post" tests may be conducted to determine reasonableness in each scenario.

Center for Internet Security Risk Assessment Method

The Center for Internet Security published a risk assessment method (*Center for Internet Security Risk Assessment Method*, or *CIS RAM*)[30] in 2018 to help organizations determine whether their application of CIS Controls would demonstrate the right cost-benefit balance. CIS RAM is based on Duty of Care Risk Analysis (DoCRA).[31]

CIS RAM's risk assessment process resembles many others, such as NIST Special Publications 800-30,[32] ISO 27005,[33] and FAIR[34] in that Risk is computed in terms of Impact and Likelihood (e.g., R= I x L). Other variations include additional factors, such as time-to-event, vulnerability, the attractiveness of the target, and other characteristics of risk.

CIS RAM requires that risk analysis also follow a set of principles that are aligned with a duty of care, and with common definitions of reasonableness. These principles are:

1. Risk analysis must consider the interests of all parties that may be harmed by the risk.
2. Risks must be reduced to a level that would not require a remedy to any party.
3. Safeguards must not be more burdensome than the risks they protect against.

This ensures that each risk analysis evaluates the potential of harm that may befall the enterprise's internal objectives (e.g., profitability), its mission (e.g., to heal patients, educate students, provide food, or manufacture goods), and its obligations to prevent harm to others (which might include preserving privacy, preventing fraud, or preventing physical harm).

CIS RAM instructs risk managers to evaluate both the current state of risk, risks associated with a recommended safeguard, and alternatives.

CIS RAM also requires an enterprise to establish a definition of risk acceptance that would be acceptable to all foreseeably harmed parties. This way, a risk manager could determine whether risks were acceptable or not. CIS RAM includes the concept of an impact "cap"—a

maximum impact assessed as low enough to require no risk mitigation.

Since its publication, CIS RAM, DoCRA, and DoCRA's principles have been cited by or used by U.S.-based regulators as methods for determining whether cybersecurity programs are reasonable. See Appendix J for specific cases.

The Sedona Conference Commentary on a Reasonable Security Test

The Sedona Conference, a nonpartisan, nonprofit organization that publishes papers and guides about technology and the law, published a paper in 2021[35] that provides a useful model for applying risk analysis when evaluating the reasonableness of protective measures. The purpose of the paper was to help adjudicators (judges, regulators, mediators, and others) determine after a data breach whether the breached organization used reasonable cybersecurity measures to protect the data. The paper suggested that a breached enterprise's liability can be argued for or against based on a two-step process:

1 Determine whether the organization applied a standard of care (for example, did they follow the CIS Controls as part of their cybersecurity program?)

2 If not, and the organization did implement some protective measures, determine if there are one or more alternate protective actions (controls or safeguards) that should have been applied commensurate with the potential risk, impact, and likelihood. If the plaintiff or regulator suggests a protective action whose added burden would have been less than the added benefit (the reduction of risk), then the inclusion of this protection action—according to the Sedona Conference paper—would not be unreasonable.

How These Testing Approaches Differ

The Sedona Conference test for reasonable security differs from CIS RAM in two significant ways.

Firstly, as a retrospective test it determines whether alternative controls would have been more reasonable than any breached control. Plaintiffs and adjudicators have an advantage of hindsight that risk managers do not enjoy prior to the incident. A risk manager may have evaluated an original control as reasonable at the time of the breach, without also evaluating every other possible control that may have had a better cost-benefit payoff.

Secondly, CIS RAM includes the concept of a cap, while the Sedona Conference paper does not.

In these ways the adjudicator's test and the risk manager's test are befitting of their roles. The risk manager looks for controls and safeguards they evaluate as reasonable, given what they know, what they foresee, and their legitimate business interests. The adjudicator's role is to determine whether unacceptable harm was avoidable within the enterprise's means.

In both cases, however, the risk manager and adjudicator acknowledge that perfect security is not achievable. Protective measures cannot always prevent harm, and enterprises cannot always implement and operate ideal protective measures. Rather than require an unattainable perfect state of security, both the legal and cybersecurity communities have turned to risk analysis to at least determine whether an enterprise applied sufficient security, given their mission, their objectives, and their obligations to others.

APPENDIX J

State Attorney General Enforcement Actions in Data Breach Lawsuits

Referencing existing guidelines and methodologies such as the Duty of Care Risk Analysis Standard (DoCRA Standard),[36] the Center for Internet Security's Risk Assessment Method (CIS RAM),[37] a tool based on the CIS Controls, which, as discussed throughout this guide, are becoming a global, de facto cybersecurity standard, and the "Sedona Conference Commentary on a Reasonable Security Test," several state Attorneys General have concluded enforcement actions against entities that suffered a data breach by requiring those entities to demonstrate reasonable security controls going forward.

Example states and cases include:

Year	Case
2021	Pennsylvania uses DoCRA and CIS RAM to define reasonable safeguards in a data breach lawsuit. *Pennsylvania v Earl Enterprises:* https://thesedonaconference.org/sites/default/files/meeting_paper/02-08.pdf
2022	Pennsylvania uses DoCRA, CIS RAM, and the Sedona Conference paper to define reasonable safeguards in a data breach lawsuit. *Pennsylvania v Hanna Andersson:* https://thesedonaconference.org/sites/default/files/meeting_paper/02-07.pdf
2022	Seven states use DoCRA's principles as a test for reasonable security in a data breach lawsuit. *Pennsylvania v Wawa.* These states include Pennsylvania, New Jersey, Delaware, Maryland, Washington D.C., Virginia, and Florida. https://thesedonaconference.org/sites/default/files/meeting_paper/02-06.pdf
2022	Two states (Pennsylvania and New York) use DoCRA, CIS RAM, and the Sedona Conference paper to define reasonable safeguards in a data breach lawsuit. *Pennsylvania v Herff Jones:* https://thesedonaconference.org/sites/default/files/meeting_paper/02-05.pdf
2023	Two states (Pennsylvania and Ohio) use DoCRA, CIS RAM, and the Sedona Conference paper to define reasonable safeguards in a data breach lawsuit. *Pennsylvania v DNA Diagnostics Center, Inc.:* https://thesedonaconference.org/sites/default/files/meeting_paper/02-04.pdf

APPENDIX K

Historical Summary of Patchwork of Federal Cybersecurity Laws and Directives

The following provides additional details about the federal cybersecurity laws and directives included in the graphical timeline in Section 3 of this paper:

In 2002, the Federal Information Security Modernization Act (FISMA) formed the basis for the protection of Federal civilian networks.[38] As amended in 2014, FISMA now requires "that agencies, in implementing their IT security programs, must follow guidance issued by OMB and standards promulgated by NIST."[39] But FISMA does *not* require agencies to implement specific cybersecurity strategies, standards, or use certain tools.[40]

Also in 2002, the Sarbanes-Oxley Act (SOX)[41] sought to protect investors by improving the accuracy and reliability of corporate disclosures made according to U.S. securities laws. SOX resulted in an increased focus on information technology controls, as these support financial processing and therefore fall into the scope of management's assessment of internal control. SOX has come to require any publicly traded company to have formal data security policies and to communicate and enforce those policies.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended by the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH), creates national standards for health care providers, health insurance plans, health care clearinghouses, and their business associates to comply with privacy and security requirements for paper and electronic medical records.[42] HIPAA does so with considerable complexity, involving a Privacy Rule, a companion Security Rule, and specific safeguards—administrative, physical, and technical—that are, in turn, composed of several standards, each of which consists of one or more implementation specifications.[43]

In 2018, Congress created the Cybersecurity and Infrastructure Security Agency (CISA),[44] which primarily serves as the lead U.S. agency to protect federal civil networks. CISA also serves as the lead federal government agency to consult and coordinate with state, local, tribal, and territorial governments as well as the private sector on issues of critical infrastructure and cybersecurity.[45]

In 2022, Congress passed the Cyber Incident Reporting for Critical Infrastructure Act, which creates significant new requirements for American critical infrastructure organizations to report cybersecurity incidents and ransom payments to the Federal government.[46]

Although other federal statutes impact cybersecurity in some way, none creates a specific minimum standard that applies to all organizations across all sectors.

Federal regulations require some organizations to comply with some cybersecurity standards further adding to the complexity

and inconsistency across the landscape. These include:

- In 1999, the Gramm–Leach–Bliley Act (GLBA)[47] changed requirements in the banking industry and, in November of 2000, pursuant to GLBA, the FTC issued the Privacy of Consumer Financial Information Rule (Privacy Rule), to address the requirements for safeguarding "nonpublic personal information."[48] The Privacy Rule requires that privacy notices provide an accurate description of current policies and practices concerning protecting the confidentiality and security of the private information.[49]

- In 2003, the FTC's "Safeguards Rule" became effective.[50] As amended, the Safeguards Rule requires financial institutions under FTC jurisdiction to have reasonable safeguards in place to keep customer information secure and to determine those safeguards through a risk assessment.[51] In October 2023, the FTC published a new amendment to the Safeguards Rule requiring financial institutions to report certain data breaches and other security events to the agency.[52] Over the years, FTC has brought many legal actions against organizations that have violated consumers' privacy rights or failed to maintain security for sensitive consumer information.[53] Supporting FISMA, the U.S. Department of Commerce, in 2006, published the Federal Information Processing Standards Publication Minimum Security Requirements for Federal Information and Information Systems (FIPS PUB 200).[54] While FISMA directed the promulgation of federal standards for minimum security requirements for information and information systems in specific categories defined within FISMA, it did not specify standards. FIPS 200 "addresses the specification of minimum security requirements for federal information and information systems."[55]

- In July 2023, the Securities and Exchange Commission (SEC) adopted rules requiring public companies to disclose all material cybersecurity incidents on a standard SEC form no later than four business days following the company's determination that the incident was material.[56] The rule also requires an annual disclosure of all cybersecurity risk management processes.[57]

- Companies that sell goods or services to the Federal government must comply with certain minimum cybersecurity standards set by Federal Acquisition Regulation (FAR), which requires government contractors to follow fifteen basic safeguarding requirements and procedures to protect systems used to collect, process, maintain, use, share, disseminate, or dispose of Federal Contract Information.[58]

- Companies that sell goods or services to the U.S. Department of Defense (DOD) may be required to comply with the minimum cybersecurity standards set by Defense Federal Acquisition Regulation Supplement (DFARS) if those products are not commercially available off the shelf.[59]

- As a final example, in 2019, the Federal Financial Institutions Examination Council (FFIEC) recommended a standardized approach to assessing cybersecurity preparedness, recommending the CIS Critical Security Controls as one of four specific tools. The FFIEC prescribes uniform principles, standards, and report forms and to promote uniformity in the supervision of financial institutions.[60]

APPENDIX L

Reasonableness Policy Checklist

The following items comprise essential policy elements an organization should perform to achieve the reasonableness guidelines presented in this guide. An organization should carefully document the steps it takes to address, implement, and maintain each of these elements. Additionally, these activities should be performed on a recurring basis to maintain an up-to-date cybersecurity program.

1. Understand the organization's mission, stakeholders, and obligations
2. Develop and implement a cybersecurity program*
3. Identify resources: funds, personnel, outsourced roles, automated tools
4. Follow an industry-recognized cybersecurity framework or standard
5. Measure conformity to the framework and mitigate findings to ensure ongoing compliance with its program
6. Conduct periodic risk assessments in accordance with methodology defined in cybersecurity program, and mitigate findings
7. Conduct periodic independent assessments of the cybersecurity program and mitigate findings

Elements of a Cybersecurity Program

- [ ] Process and criteria for identifying and protecting information of the same type addressed in the data protection law
- [ ] Roles and responsibilities
- [ ] Internal policies and enforcement requirements
- [ ] Regular cybersecurity training and awareness for personnel
- [ ] Risk methodology (includes harm to organization and harm to others; establishes a basis to either accept or mitigate risk findings)
- [ ] Process and policies for maintaining a "secure" state (e.g., software updates, removing unnecessary software, and privileged account management)
- [ ] Data recovery process

Appendix H provides a full list of security controls and their underlying actions.

Endnotes

1 Readers will note that the terms data privacy, data security, information security, and cybersecurity are used throughout the paper. These terms are related; in fact, the existence of multiple terms is a consequence of the complicated, evolving digital communication environment. However, there are subtle differences between most of them. Definitions are provided in Appendix A.

2 Center for Internet Security [CIS]. CIS Critical Security Controls. Retrieved from https://www.cisecurity.org/controls

3 Virginia Consumer Data Protection Act. Va. Code § 59.1-578(A)(3) (emphasis added). Retrieved from Virginia Law Code: https://law.lis.virginia.gov/vacodefull/title59.1/chapter53/

4 Buckbee, M. (2023, June 16). What the H**L Does Reasonable Data Security Really Mean? [Author's blog post]. Varonis Blog/Privacy & Compliance. Retrieved from https://www.varonis.com/blog/what-the-hl-does-reasonable-data-security-really-mean

5 The Sedona Conference, Commentary on a Reasonable Security Test, 22 SEDONA CONF. J. 345 (2021). Retrieved from https://thesedonaconference.org/sites/default/files/publications/5_Reasonable_Security_Test_0.pdf

6 Center for Internet Security. CIS Risk Assessment Model (CIS RAM) Version 2.1 [Course material]. https://learn.cisecurity.org/cis-ram

7 Cyber Incident Reporting for Critical Infrastructure Act. (March 15, 2022). In Consolidated Appropriations Act (Public Law 117-103). [Legislation]. Retrieved from https://www.congress.gov/117/plaws/publ103/PLAW-117publ103.pdf DHS CISA has begun to develop corresponding regulations: See CISA fact sheet retrieved from https://www.cisa.gov/sites/default/files/2022-11/Sharing_Cyber_Event_Information_Fact_Sheet_FINAL_v4.pdf

8 See National Conference of State Legislatures, Security Breach Notification Laws (updated January 17, 2022) retrieved from https://www.ncsl.org/technology-and-communication/security-breach-notification-laws

9 National Conference of State Legislatures. (n.d.). Security breach notification laws. Retrieved from NCSL website: https://www.ncsl.org/technology-and-communication/2022-security-breach-legislation. See also Privacy Rights Clearinghouse. (2023). United States data breach notification laws 2023 report. [Report.] Retrieved from https://privacyrights.org/resources/united-states-data-breach-notification-united-states-2023-report

10 201 Mass. Reg. 17.03. 201 CMR 17.00: Standards for the protection of personal information of residents of the Commonwealth. Retrieved from https://www.mass.gov/regulations/201-CMR-1700-standards-for-the-protection-of-personal-information-of-ma-residents

11 See New York State Department of Financial Services. (2023, November 1). Second amendment to 23 NYCRR 500 [Second Amendment to Part 500 Cybersecurity Requirements for Financial Services Companies]. Retrieved from https://www.dfs.ny.gov/system/files/documents/2023/10/rf_fs_2amend23NYCRR500_text_20231101.pdf

12 Cybersecurity Bankers Association [CSBA]. (2017). *Cybersecurity 101: A resource guide for financial sector executives.* Retrieved from https://www.csbs.org/sites/default/files/cybersecurity101_2019_final_with_links.pdf The Guide recommends the CIS Critical Security Controls.

13 Federal Communication Commission. (2022). Notice of proposed rulemaking [FCC 22-83] (pp. 13-14) (recommending the CIS Critical Security Controls as one of two standards). Retrieved from https://docs.fcc.gov/public/attachments/FCC-22-82A1.pdf

14 See, e.g., Deloitte. (2016). *Beneath the surface of a cyberattack: A deeper look at business impacts.* [Report]. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-risk-beneath-the-surface-of-a-cyber-attack.pdf

15 California Department of Justice, Office of the Attorney General. (2016). California data breach report. Retrieved from https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf.

16 Nevada Revised Statutes [NRS] § 603A.210. (2019). Retrieved from https://www.leg.state.nv.us/nrs/nrs-603a.html

17 Ohio Revised Code § 1354.01-1354.05 [Sections 1354.01-1354.05]. (2018). Retrieved from https://codes.ohio.gov/ohio-revised-code/section-1354.01

18 Id.

19 See, e.g., id.

20 National Institute of Standards and Technology [NIST]. (2020, September). *Security and privacy controls for information systems and organizations* (Special Publication 800-53, Rev. 5). Retrieved from https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

21 Payment Card Industry Security Standards Council. (n.d.). PCI Data Security Standard [PCI DSS]. Retrieved from https://www.pcisecuritystandards.org/standards/

22 International Organization for Standardization [ISO]. (2022). *ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on information security risk management (4th ed.)*. Retrieved from https://www.iso.org/standard/80585.html

23 Verizon Data Breach Investigations Report. https://www.verizon.com/business/resources/reports/dbir/

24 *Blueprint for Ransomware Defense: An Action Plan for Ransomware Mitigation, Response, and Recovery.* Institute for Security and Technology, 2022. https://securityandtechnology.org/ransomwaretaskforce/blueprint-for-ransomware-defense/

25 Center for Internet Security [CIS]. (2021). CIS Community Defense Model v2.0. Retrieved from https://www.cisecurity.org/insights/white-papers/cis-community-defense-model-2-0

26 Id.

27 Id.

28 *The Cost of Cyber Defense: Implementation Group 1.* Center for Internet Security, 2023. https://learn.cisecurity.org/l/799323/2023-08-02/4t3qkj/799323/1694810927NC0iZQGR/CIS_Controls__Cost_of_Cyber_Defense__2023_08.pdf

29 *CIS Critical Security Controls Navigator.* Center for Internet Security (updated regularly). https://www.cisecurity.org/controls/cis-controls-navigator/

30 Center for Internet Security. (n.d.). CIS Risk Assessment Method (CIS RAM). Retrieved from https://learn.cisecurity.org/cis-ram

31 The DoCRA Council. (2021). Duty of Care Risk Analysis [DoCRA] Standard v 0.6 [Document]. Retrieved from https://www.docra.org/wp-content/uploads/2021/06/Duty-of-Care-Risk-Analysis-Standard-Draft-20200907.pdf

32 National Institute of Standards and Technology (NIST). (2012). Guide for conducting risk assessments (NIST Special Publication 800-30 Rev. 1). Retrieved from https://csrc.nist.gov/pubs/sp/800/30/r1/final

33 International Organization for Standardization (ISO). (2022). ISO/IEC 27005: Information security, cybersecurity and privacy protection – Guidance on managing information security risks. [ISO Standards] Retrieved from https://www.iso.org/standard/80585.html

34 Factor Analysis of Information Risk (FAIR). [The FAIR Institute]. Retrieved from https://www.fairinstitute.org/what-is-fair

35 The Sedona Conference, Commentary on a Reasonable Security Test, 22 SEDONA CONF. J. 345 (2021). https://thesedonaconference.org/sites/default/files/publications/5_Reasonable_Security_Test.pdf

36 The DoCRA Council. (2021). Duty of Care Risk Analysis [DoCRA] Standard v 0.6 [Document]. Retrieved from https://www.docra.org/wp-content/uploads/2021/06/Duty-of-Care-Risk-Analysis-Standard-Draft-20200907.pdf

37 Center for Internet Security. (n.d.). CIS Risk Assessment Method (CIS RAM). Retrieved from https://learn.cisecurity.org/cis-ram

38 See Federal Information Security Management Act of 2002. In E-Government Act of 2002, Public Law 107-347. Retrieved from https://www.congress.gov/107/plaws/publ347/PLAW-107publ347.pdf

39 Congressional Research Service [CRS]. (2021, September 29). Federal cybersecurity: Background and issues for Congress [Report No. R46926]. Retrieved from https://crsreports.congress.gov/product/pdf/R/R46926 See Federal Information Security Modernization Act of 2014, Public Law 113-283. Retrieved from https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf

40 Id.

41 See Sarbanes-Oxley Act of 2002, Public Law No. 107-204. Retrieved from https://www.congress.gov/107/plaws/publ204/PLAW-107publ204.pdf

42 Congressional Research Service [CRS]. (Updated 2015, April 17). HIPAA Privacy, Security, Enforcement, and Breach Notification Standards," [Report No. R43991.] Retrieved from https://crsreports.congress.gov/product/pdf/R/R43991. See the Health Insurance Portability and Accountability Act of 1996, Public Law No. 104-191. Retrieved from https://www.congress.gov/104/plaws/publ191/PLAW-104publ191.pdf

43 Id.

44 Cybersecurity and Infrastructure Security Agency Act of 2018, Public Law No. 115-278. Retrieved from https://www.congress.gov/bill/115th-congress/house-bill/3359/text

45 Id. at Section 2202 (e) (1) (I) and (N). See also DHS CISA Cyber Mission Overview: https://www.dhs.gov/news/2022/10/03/cyber-mission-overview

46 Cyber Incident Reporting for Critical Infrastructure Act, Public Law No. 117-103 (2022, March 15). In Consolidated Appropriations Act, 2022 (H.R. 2471, 117th Cong.) Retrieved from https://www.congress.gov/117/plaws/publ103/PLAW-117publ103.pdf

47 Gramm-Leach-Bliley Act (GLBA), Public Law 106-102 (1999). Retrieved from https://www.govinfo.gov/content/pkg/PLAW-106publ102/html/PLAW-106publ102.htm

48 Federal Trade Commission. (2000). Privacy of consumer financial information (16 C.F.R. Part 313). Retrieved from https://www.ftc.gov/legal-library/browse/rules/financial-privacy-rule

49 Federal Trade Commission (FTC), "How To Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act" [FTC website]. Retrieved from https://www.ftc.gov/business-guidance/resources/how-comply-privacy-consumer-financial-information-rule-gramm-leach-bliley-act

50 Federal Trade Commission. (2021, December 9). Standards for safeguarding customer information (16 CFR Part 314) [Revision of rule]. Federal Register, 86(236), 70272-70312. Retrieved from https://www.ftc.gov/system/files/ftc_gov/pdf/p145407_safeguards_rule.pdf

51 Id.

52 Federal Trade Commission. (2021, December 9). Standards for safeguarding customer information (16 CFR Part 314) [Revision of rule]. Federal Register, 86(236), 70272-70312. Retrieved from https://www.ftc.gov/system/files/ftc_gov/pdf/p145407_safeguards_rule.pdf

53 Federal Trade Commission (FTC). (n.d.). Privacy and security enforcement [Topic page]. Retrieved from https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement

54 National Institute of Standards and Technology (NIST). (2006). Federal Information Processing Standards (FIPS) Publication 200: *Minimum Security Requirements for Federal Information and Information Systems.* Retrieved from https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.200.pdf

55 Id.

56 See Securities and Exchange Commission. (2023, July 26). Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure [Final rule]. Federal Register, 88(144), 41900-41940. Retrieved from https://www.sec.gov/rules/final/2023/33-11216.pdf

57 Id.

58 Federal Acquisition Regulation (FAR) [Subpart 52.204-21, Basic safeguarding of covered contractor information systems]. Retrieved from https://www.acquisition.gov/far/52.204-21

59 Defense Federal Acquisition Regulation Supplement [DFARS]. (2018, December 20). 252.204-7012: Safeguarding covered defense information and cyber incident reporting. Retrieved from https://business.defense.gov/Portals/57/Safeguarding%20Covered%20Defense%20Information%20-%20The%20Basics.pdf

60 Federal Financial Institutions Examination Council [FFIEC]. (2019, August 28). FFIEC encourages standardized approach to assessing cybersecurity preparedness [Press release]. Retrieved from https://www.ffiec.gov/press/pr082819.htm

The Center for Internet Security, Inc. (CIS®) makes the connected world a safer place for people, businesses, and governments through our core competencies of collaboration and innovation. We are a community-driven nonprofit, responsible for the CIS Critical Security Controls® and CIS Benchmarks™, globally recognized best practices for securing IT systems and data. We lead a global community of IT professionals to continuously evolve these standards and provide products and services to proactively safeguard against emerging threats. Our CIS Hardened Images® provide secure, on-demand, scalable computing environments in the cloud.

CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities, and the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®), which supports the rapidly changing cybersecurity needs of U.S. election offices.

www.cisecurity.org
info@cisecurity.org
518-266-3460
Center for Internet Security
@CISecurity
CenterforIntSec
TheCISecurity
cisecurity

Center for Internet Security® | CIS Controls™