Harmonizing U.S. Cybersecurity Regulations: Opportunities & Challenges

Josephine Wolff
Josephine.Wolff@Tufts.edu

Fletcher School of Law and Diplomacy
Tufts University

Hitachi Center for Technology & International Affairs Working Paper
November 2024

FLETCHER
HITACHI CENTER FOR TECHNOLOGY
& INTERNATIONAL AFFAIRS

Introduction

While regulators in the United States have been paying increasing attention to cybersecurity in recent years, their efforts to design policies have often been uncoordinated and specific to their industry sector, state, or agency. As a result, while U.S. cybersecurity regulations have proliferated, many of those regulations impose different requirements for security, or use different language to address related risks and mitigations. This has led to a complicated patchwork of different regulations that are in some cases duplicative or overlapping, in some cases directly contradictory, and in many cases subtly different in their language in ways that can make it difficult for regulated entities to determine how to comply with all of them. These subtle and not-so-subtle differences in overlapping cybersecurity regulations can create burdens not just for regulated entities, who have to figure out how to comply with all of them, but also for regulators, who are tasked with developing novel security standards and enforcement regimes over and over again to address the same set of risks. In both cases, there is a risk that investing additional time and personnel in trying to navigate complicated, overlapping compliance requirements or enforcement processes may detract from the overall cybersecurity objectives of both regulated entities and regulators by dividing their attention and resources instead of allowing them to focus on a single, clear set of cybersecurity requirements and standards.

To address this concern that disparate, differentiated cybersecurity regulations might actually undermine overall cybersecurity efforts, the 2023 National Cybersecurity Strategy highlighted the need to "harmonize and streamline new and existing regulations" as one of the objectives for better defending critical infrastructure. The strategy states: "Where Federal regulations are in conflict, duplicative, or overly burdensome, regulators must work together to minimize these harms."[1] However, the Strategy did not specify which regulations were in conflict, duplicative, or overly burdensome and untangling the existing set of sprawling cybersecurity regulations to identify these areas of discrepancy and overlap is far from straightforward given both how many cybersecurity-related regulations there are across the United States and that many of them apply only to specific industry sectors, states, or government agencies.

To help surface some possible areas for harmonization, the Office of the National Cyber Director (ONCD) posted a Request for Information (RFI) in August 2023 soliciting input about cybersecurity regulations related to critical infrastructure and asking respondents to, among other things, "provide examples of any conflicting, mutually exclusive, or inconsistent Federal and SLTT [state, local, Tribal, and territorial] regulations affecting cybersecurity — including broad enterprise-wide requirements or specific, targeted requirements — that apply to the same information technology (IT) or operational technology (OT) infrastructure of the same regulated entity."[2] ONCD received 86 responses to the RFI and in June 2024 released a summary of the comments, concluding that (1) "The lack of harmonization and reciprocity harms cybersecurity outcomes while increasing compliance costs through additional administrative burdens; (2) "Challenges with cybersecurity regulatory harmonization and reciprocity extend to businesses of

[1] United States National Cybersecurity Strategy, March 2023. Available from https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

[2] Request for Information on Cyber Regulatory Harmonization; Request for Information: Opportunities for and Obstacles To Harmonizing Cybersecurity Regulations. August 16, 2023. Available from https://www.federalregister.gov/documents/2023/08/16/2023-17424/request-for-information-on-cyber-regulatory-harmonization-request-for-information-opportunities-for.

all sectors and sizes" and (3) "The U.S. Government is positioned to act to address these challenges."[3]

This report builds on that analysis by ONCD, as well as related assessments by the Government Accountability Office (GAO), the Congressional Research Service, and others, to tackle two broad questions related to harmonizing U.S. cybersecurity regulations:

1. What are the differences between existing U.S. guidance, rules, and regulations governing reporting of cybersecurity incidents and minimum cybersecurity controls for organizations, especially at the federal level?
2. Which of these differences provide the greatest potential opportunity for harmonization and what are the advantages and disadvantages of harmonizing around each of the different variations that have been tried?

These questions are fundamental to undertaking any harmonization effort, and despite the government's ongoing focus on harmonization, they remain largely unanswered, even in many of the RFI responses.

There are several other areas of regulatory harmonization that are worth considering, including the harmonization of approval processes for acquisitions, alignment with international standards, and reciprocity. While some of these relate to issues of incident reporting and minimum cybersecurity controls, they also encompass broader questions linked to harmonization beyond the borders of the United States and which authorities are trusted to assess the cybersecurity level of different services and products. For the purposes of this paper, we focus on cybersecurity controls and incident reporting both because these are integral to cybersecurity regulations across every sector and level of government, and because without consistency around these issues—particularly baseline controls—it will be more challenging to achieve harmonization around issues of approvals, reciprocity, and international standards alignment.

This report is organized according to three areas of discrepancy in cybersecurity regulations: definitions, security controls, and reporting requirements. The first section looks at how different regulations define central terms and ideas such as a cybersecurity incident, data breach, or personal data. These definitions are crucial for harmonization because even if two regulations purport to do the same thing—for instance, require reporting of cybersecurity incidents or protection of sensitive data—their requirements may be quite different in practice if they define incidents or sensitive data differently. The next section looks at discrepancies in the security controls and practices required by different regulations, specifically around use of multi-factor authentication, encryption, firewalls and network segmentation, and audits and testing. The following section examines discrepancies in incident reporting requirements, specifically reporting timelines, whom incidents must be reported to, and what information must be reported. The final section considers which of the identified discrepancies could be most feasibly and usefully harmonized and the advantages and disadvantages of different approaches to doing so.

Two cross-cutting concerns come up in discussions of cybersecurity regulatory harmonization that apply to all of these topics. One is a fear that harmonization could lead to lower baseline

[3] Office of the National Cyber Director, Summary of the 2023 Cybersecurity Regulatory Harmonization Request for Information, June 2024. Available from https://www.whitehouse.gov/wp-content/uploads/2024/06/Cybersecurity-Regulatory-Harmonization-RFI-Summary-ONCD.pdf.

security requirements if regulated entities currently feel they must abide by the requirements of the most stringent regulation they are subject to but that regulation is eliminated or pre-empted by a less stringent one in the name of harmonization. As the International Information System Security Certification Consortium (ISC2) put it in their response to the ONCD RFI, "organizations faced with overlapping, redundant, and/or conflicting cybersecurity requirements look to the 'highest watermark,' or said another way, the most restrictive requirements under each applicable law or regulation."[4]

A second concern is that harmonization could lead to a one-size-fits-all approach to cybersecurity in which all industries are regulated in the same manner regardless of their different threat models, risk profiles, and infrastructure. For instance, in its response to the ONCD RFI, the Aerospace Industries Association notes, "it is imperative that aerospace-specific standards are developed and used to efficiently manage risks in a manner suitable to the operating environment. With such tailored standards, cybersecurity risks can be adequately mitigated even if it does not follow the common practices seen elsewhere."[5] ONCD, in its RFI, sought to allay some of these concerns by noting that its notion of harmonization "refers to a common set of updated baseline regulatory requirements that would apply across sectors. Sector regulators could go beyond the harmonized baseline to address cybersecurity risks specific to their sectors."[6] This analysis aims in part to assess the feasibility of this tiered sector-specific approach to harmonization and to understand where it may be most possible to align requirements across different industries and where there may be a need for more custom tailoring of policies, or more stringent baseline security expectations.

Opportunities for Harmonization: Definitions

This analysis focuses on two broad types of cybersecurity regulations: those that impose baseline security requirements for protecting computer networks and data, and those that require reporting of certain types of security incidents. However, across both types of regulations there is another set of preliminary harmonization issues in the form of how regulations define fundamental ideas about what constitutes a security incident and what types of data and computer systems require protection. This section considers some of the discrepancies in those definitions, offering potential areas for harmonizing these critical concepts even before trying to harmonize the requirements about how they should be reported or protected. Without some degree of standardization of these definitions, it will be impossible to meaningfully harmonize different cybersecurity regulations regardless of how aligned their requirements may otherwise be.

[4] ISC2, Request for Information: Opportunities for and Obstacles to Harmonizing Cybersecurity Regulations, October 31, 2023. Available from https://www.regulations.gov/comment/ONCD-2023-0001-0056.

[5] Aerospace Industries Association, Request for Information: Opportunities for and Obstacles to Harmonizing Cybersecurity Regulations: Docket No. ONCD-2023-0001. Available from https://www.regulations.gov/comment/ONCD-2023-0001-0073.

[6] Request for Information on Cyber Regulatory Harmonization; Request for Information: Opportunities for and Obstacles To Harmonizing Cybersecurity Regulations. August 16, 2023. Available from https://www.federalregister.gov/documents/2023/08/16/2023-17424/request-for-information-on-cyber-regulatory-harmonization-request-for-information-opportunities-for.

There are a variety of different terms used and defined in cybersecurity regulation that provide opportunities for harmonization, including data breaches, pseudonymization, cyber risk, cyber threat, and cybersecurity plans. This section considers two sets of definitions—those for cybersecurity incidents, and for personal information—where there is particularly significant variation across regulations, but similar analysis could be applied to a broader set of definitions in the future.

Defining Cybersecurity Incidents

One of the fundamental questions for establishing reporting or liability requirements related to cybersecurity incidents is the question of what, precisely, constitutes an incident. This is an especially pertinent question for the wide range of cybersecurity incident and breach reporting regulations that have emerged in recent years, many of which define what, specifically, needs to be reported under their requirements in slightly—or in some cases, significantly—different terms.[7] As the Insurance Coalition pointed out in its response to the ONCD RFI:

> The definition of 'cybersecurity incident,' 'cybersecurity event,' or analogous term under Cybersecurity Rules is inconsistent. The occurrence of a cybersecurity incident generally triggers many obligations and can result in significant liability, penalties, or fines on the covered entity, and therefore, it is critically important for covered entities to i) understand if and when its obligations under the applicable law or regulation are triggered and ii) operationalize compliance with each applicable law and regulation.[8]

Different regulators and standards-setting bodies have taken different approaches to defining incidents, as shown in Table 1.

Table 1: Different definitions of cybersecurity incidents in regulations, rules, and standards.

Source	Definition of Cybersecurity Incident
CIRCIA	"An occurrence that actually jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system; or actually jeopardizes, without lawful authority, an information system"
TSA Security Directive Pipeline-2021-01B	"An event that, without lawful authority, jeopardizes, disrupts or otherwise impacts, or is reasonably likely to jeopardize, disrupt or otherwise impact, the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident on the system. This definition includes an event that is under investigation or evaluation by the owner/operator as a possible cybersecurity incident without final determination of the event's root cause or nature (such as malicious, suspicious, benign)."
OMB M-17-12	"An occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an

[7] Mary Brooks and Sofia Lesmes, "Cybersecurity Incident and Breach Reporting Requirements," R Street. June 23, 2022. Available from https://www.rstreet.org/commentary/cybersecurity-incident-and-breach-reporting-requirements/.

[8] The Insurance Coalition, October 31, 2023. Available from https://www.regulations.gov/comment/ONCD-2023-0001-0020.

	information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies”
SEC Cybersecurity Rule	“An unauthorized occurrence, or a series of related unauthorized occurrences, on or conducted through a registrant’s information systems that jeopardizes the confidentiality, integrity, or availability of a registrant’s information systems or any information residing therein”
FTC Safeguards Act	“An event resulting in unauthorized access to, or disruption or misuse of, an information system, information stored on such information system, or customer information held in physical form.”
HIPAA	“The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system”
NIST FIPS Pub 200	“An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.”
ISO 27000	“A single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security”
NYDFS Cybersecurity Regulation	“Any act or attempt, whether successful or not, to gain unauthorized access to, disrupt, or misuse an information system or information stored on such system.”

Some of the differences across these definitions may be merely semantic—though even in those cases, parsing the subtle differences in language may add to the compliance burden for regulated entities. In such cases, harmonization may be relatively simple, a matter of agreeing on a standard definition rather than actually navigating substantially different approaches to regulation. However, other differences in these definitions are clearly substantive and significant. For instance, some of these regulations include events in which computer systems are not actually accessed by intruders. For instance, the NYDFS definition includes “any act or attempt, *whether successful or not*, to gain unauthorized access,” the HIPAA definition includes “*attempted* … unauthorized access,” and the TSA definition which includes not just incidents that that are only “reasonably likely” to disrupt computer systems but also all incidents that are still under investigation, for which the regulated entity has not yet determined how or why they occurred. By contrast, CIRCIA defines incidents as events that *actually* jeopardize information systems, explicitly excluding ones that “imminently” jeopardize such systems. The SEC and FTC take similar approaches, predicating their definitions, respectively, on information systems being jeopardized or successful acts of unauthorized access.

There are three related but distinct components that appear in these definitions as thresholds for the definition of a cybersecurity incident: (1) unauthorized access to computer systems, (2) jeopardizing the confidentiality, integrity, or availability of information or an information system, and (3) violation of security policies. Often, as shown in Table 1, a definition may include more than one of these components to allow for the broadest possible set of incidents—for instance, it may be possible to jeopardize the availability of a session without gaining unauthorized access to it, as in the case of many denial-of-service attacks. Similarly, not every act of unauthorized access necessarily leads to the compromise of confidentiality, integrity, or availability of computer systems. Additionally, violations of security policies may not require unauthorized access or the compromise of confidentiality, integrity, or availability to occur.

In addition to selecting which threshold components, they wish to include, regulators must also make a decision about how certain organizations must be about the occurrence of each of these components in order to trigger an incident reporting obligation. A definition may require that the particular threshold it specifies (1) definitely occurred, (2) definitely was attempted, (3) may have occurred with some "reasonable likelihood," or (4) may be about to occur as an "imminent threat." In developing their definitions of cybersecurity incidents, in other words, regulators must first choose which types of events they wish to include (acts of unauthorized access, acts that jeopardize confidentiality, integrity, or availability, or acts that violate security policies) and then, for each of the categories of events they include, they can then decide with what degree of certainty those events must occur to trigger the associated regulatory requirements. This range of different incident thresholds and levels of certainty has contributed to the variety of incident definitions currently populating cybersecurity regulations, making it difficult to parse exactly when a potential security issue escalates to the point where a report is required.

Harmonizing definitions of cybersecurity incidents would require making a choice as to whether or not the standard definition should include potential, imminent, or unsuccessful incidents that may be under investigation or never have resulted in any actual compromise. In general, it would seem most straightforward to harmonize such definitions around one of the templates that requires an actual compromise to have occurred, if only because there is less ambiguity in identifying such events than in trying to determine when unsuccessful or potential incidents have occurred. Certain regulators may still choose to expand their definition if, for instance, they believe that even unsuccessful attempts to penetrate computer systems warrant scrutiny or investigation given the sensitivity or risk profile of their respective industry sectors. In doing so, however, they may need to offer clearer guidelines about how to identify imminent, unsuccessful, and potential security events in a consistent manner. It may even make more sense to define such events as a separate category from security incidents (something along the lines of "near misses" or "attempted intrusions")—both to enable harmonization of the definition of a security incident and to differentiate between successful and unsuccessful security compromises.

Consistent definitions would not necessarily require every sector to implement identical reporting requirements for cybersecurity incidents—it may be the case that for some sectors it is especially helpful to have data on imminent incidents, while for others it is not. However, consistent definitions would enable a tiered system in which broad reporting requirements like CIRCIA or the SEC rules, which apply to a wide range of sectors, could apply to a core tier of incidents that actually occur and jeopardize confidentiality, integrity, or availability. Individual sectors could then decide whether to build on those regulations with additional requirements related to tiers of imminent, possible, or attempted incidents that cross other thresholds (e.g., violation of security policies or unauthorized access) of particular relevance to them.

Defining Personal Information

Another source of divergence among cybersecurity regulations is how they define the categories of personal information that require protection or that must be reported if breached. Table 2 shows some different definitions of the types of personal information that cybersecurity regulations apply to in different contexts.

Table 2: Different definitions of personal information in cybersecurity regulations, rules, and standards.

Source	Definition of Personal Information
CIRCIA	"Information that identifies a specific individual or nonpublic information associated with an identified or identifiable individual. Examples of personal information include, but are not limited to, photographs, names, home addresses, direct telephone numbers, social security numbers, medical information, personal financial information, contents of personal communications, and personal web browsing history."
OMB (FedRAMP) and NIST 800-63	"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"
FTC Safeguards Rule	"Personally identifiable financial information means any information: (i) A consumer provides to you to obtain a financial product or service from you; (ii) About a consumer resulting from any transaction involving a financial product or service between you and a consumer; or (iii) You otherwise obtain about a consumer in connection with providing a financial product or service to that consumer."
HIPAA	"Individually identifiable health information is information that is a subset of health information, including demographic information collected from an individual, and: (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (i) That identifies the individual; or (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual."
FERPA	"Information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty"
COPPA	"Individually identifiable information about an individual collected online, including— (A) a first and last name; (B) a home or other physical address including street name and name of a city or town; (C) an e-mail address; (D) a telephone number; (E) a Social Security number; (F) any other identifier that the Commission determines permits the physical or online contacting of a specific individual; or (G) information concerning the child or

	the parents of that child that the website collects online from the child and combines with an identifier described in this paragraph.”
Gramm-Leach-Bliley Act	“ ‘Nonpublic personal information’ means personally identifiable financial information— (i) provided by a consumer to a financial institution; (ii) resulting from any transaction with the consumer or any service performed for the consumer; or (iii) otherwise obtained by the financial institution. … Such term does not include publicly available information”
FCC	“Customer proprietary network information (CPNI) in the carriers' possession … includes: the location of an active mobile device; the phone numbers called by a consumer; the frequency, duration, and timing of such calls; and any services purchased by the consumer, such as call waiting.”
ISO 27002	“Any piece of information that confirms an individual's identity”
CCPA	“Information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.”
GDPR	“Any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person”

As with the definitions of cybersecurity incidents, the definitions of personal information demonstrate both some seemingly superficial differences and some substantive ones. For instance, the definitions in the FTC Safeguards Rule and the Gramm-Leach-Bliley are almost the same, while those in OMB M-17-12 (which is also used for the FedRAMP designation) and NIST 800-63 are identical and related to but slightly different from that in CIRCIA. One of the crucial differences among these definitions include whether personal data must be nonpublic in nature, or whether it applies to any information that could be linked to an individual. Meanwhile, several regulations, such as FERPA, HIPAA, the FTC, and the FCC rules on CPNI have definitions tailored to their particular industry sectors (education, health, consumer protection, and telecommunications).

These sector-specific definitions may make sense in some cases, as in the FCC’s designation of location and call data as requiring protection, since those categories would be irrelevant in many other contexts, but there may still be an opportunity for baseline harmonization around a definition of personal data that could then be augmented with sector-specific data categories. The COPPA definition, for instance, lists several categories of information that apply generally, not just to children’s Internet usage, such as names, addresses, telephone numbers and social security numbers, and then adds to those categories additional data that might be collected through a child’s online activities and combined with those other identifiers. This would seem like a plausible model for other more targeted regulations—to establish a baseline definition of personal data and then designate other information collected in combination with that data as personal.

Clarifying the definition of personal data in this manner could substantially ease the burden of compliance on regulated entities that deal with different types of data across different sectors. Business Roundtable, in its response to ONCD's RFI, highlighted this compliance burden, noting, "Definitions of several protected data types — including sensitive personal information, protected health information and personally identifiable information — vary significantly by state and by agency. For example, depending on the state, health records may or may not qualify as sensitive personal information. This means that cybersecurity solutions for the same data may be compliant with certain regulations or contracts but not others."[9] The Insurance Coalition also noted the challenges of trying to apply different regulatory regimes to the same data depending on whether it falls under the definitions of different rules.

Defining Pseudonymous & Deidentified Data

Notably, harmonizing definitions of personal information might also enable greater harmonization of definitions for pseudonymous and deidentified data. For instance, Cooperative Exchange, the National Clearing House Association, in its response to the 2023 RFI, notes the differences between the HIPAA and CCPA requirements for designating data as deidentified. HIPAA defines deidentified data as health information that "does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual." The CCPA builds on that definition, adding additional requirements that a business designating data as deidentified must also take "reasonable measures to ensure that the information cannot be associated with a consumer or household," and publicly commit to "maintain and use the information in deidentified form and not to attempt to reidentify the information, except … for the purpose of determining whether its deidentification processes satisfy the requirements of" the law, and additionally contractually obligate all recipients of the information to do the same. Interestingly, the definitions of pseudonymization in the CCPA and the GDPR are much more closely aligned, using almost exactly the same language, suggesting that there is more consensus around the meaning of pseudonymous data than deidentified data.

Taken together, these different definitions suggest both that there is considerable alignment around the underlying ideas and language for many of these notions of cybersecurity incidents and personal data, but also that there are some crucial decisions that must be made about what is and is not included in these categories to more forward with more effective harmonization efforts. For instance, just deciding whether or not cybersecurity incidents include unsuccessful or imminent compromises and whether or not personal data includes public information that can be linked to individuals would already be a major step towards harmonizing these definitions across different regulations.

Opportunities for Harmonizing Definitions

Three key questions around harmonizing cybersecurity definitions emerge from this review of existing cybersecurity regulations: (1) What types of events count as cybersecurity incidents? (2)

[9] Business Roundtable, "Comments of Business Roundtable on the Request for Information on Cybersecurity Regulatory Harmonization," October 12, 2023. Available from https://www.regulations.gov/comment/ONCD-2023-0001-0009.

How certain does someone need to be that the event occurred for it to be considered an incident? And (3) Does personal data have to be nonpublic for it to trigger reporting requirements? In this section, we consider briefly the potential answers to each of these questions as well as the advantages and disadvantages of each option, and the rationale for allowing some variation across different sectors' answers.

Harmonization Question #1: What types of events count as cybersecurity incidents?

- Option #1.1: Acts of unauthorized access to a computer system
    - Advantages: Includes broad set of incidents that do not have clear impacts related to confidentiality, integrity or availability, enabling broader collection of data on intrusions and system vulnerabilities.
    - Disadvantages: Acts of unauthorized access may be difficult to detect and in some cases may not pose a significant threat to cybersecurity, leading to overreporting.
- Option #1.2: Acts that jeopardize the confidentiality, integrity, or availability of a computer systems or data stored on a computer system
    - Advantages: Focuses on impacts of an incident, thereby limiting reporting to events that have a real effect on systems or data; clear definition of what it means when an event reaches this threshold.
    - Disadvantages: May enable less data collection on intrusions and other events that have minimal or no impact.
- Option #1.3: Acts that violate security policies
    - Advantages: Could potentially encompass an even broader set of events and greater data collection.
    - Disadvantages: Leaves organizations a fairly broad remit to define their own security policies, leading to potential inconsistencies in reporting.
- Rationale for variation across industry sectors: Different sectors may feel they need access to information about less impactful events depending on the risk level associated with access or violation of security policies.
- Recommended baseline definition: Option #1.1 (with opportunity to extend it by adding options 1.2 or 1.3 as needed, with relevant justification)

Harmonization Question #2: How certain does someone need to be that the event occurred for it to be considered an incident?

- Option #2.1: Only include successful/actual compromises that have definitely occurred
    - Advantages: Clear, can be consistently applied by all organizations, limits data collection to actual incidents.
    - Disadvantages: May mean foregoing access to useful aggregate information about near misses.
- Option #2.2: Include attempted compromises
    - Advantages: Provides an opportunity to learn from near misses and circumstances where security controls performed well.
    - Disadvantages: Unclear what constitutes an "attempt" which may lead to inconsistent interpretations and reporting by different organizations.
- Option #2.3: Include events that are "reasonably likely" to have occurred or are under investigation

    - Advantages: Makes it more difficult for organizations to avoid reporting incidents when forensic evidence of a compromise is difficult to gather.
    - Disadvantages: May detract from organizations' focus on their investigations; may result in overreporting about incidents that do not turn out to be malicious or intentional; may lead to inconsistent interpretations of "reasonable likelihood" and inconsistent reporting by different organizations.
- Option #2.4: Include events that there is an imminent threat of being about to occur
    - Advantages: May enable rapid response and mitigation of imminent threats by regulators.
    - Disadvantages: Unclear what constitutes an "imminent threat" of an incident, which may lead to inconsistent interpretations and reporting by different organizations; may result in overreporting of incidents that are not important.
- Rationale for variation across industry sectors: Different sectors may feel they need access to information about less certain incidents or near misses in order to compile better data on the effectiveness of safeguards or how best to prevent compromises.
- Recommended baseline definition: Option #2.1 (with opportunity to extend it by adding options 2.2, 2.3, or 2.4 as needed, with relevant justification)

Harmonization Question #3: Does personal data have to be nonpublic for it to trigger reporting requirements?

- Option #3.1: To qualify as personal data information must be nonpublic
    - Advantages: Avoids organizations having to report breaches of public information that have minimal or no impact.
    - Disadvantages: Some public information may still be worth protecting, especially if stored together with other information.
- Option #3.2: Public information can be personal data if it is possible to link to an individual
    - Advantages: Eliminates ambiguity around determining whether information is public or not.
    - Disadvantages: Requires organizations to expend resources protecting information that may be freely available to all.
- Rationale for variation across industry sectors: Different sectors deal with different types of information and may want to tailor their regulations to those specific types of data.
- Recommended baseline definition: Option #3.1 (with opportunity to extend it by adding option 3.2 as needed, with relevant justification)

Opportunities for Harmonization: Security Controls & Practices

In addition to different definitions regarding which type of data needs to be protected, cybersecurity regulations also impose a variety of different security requirements and controls for the purpose of that protection. This section considers the two categories of safeguards that are referenced in the largest number of U.S. regulations analyzed, specifically multi-factor authentication (MFA) and encryption, as well as some discussion of other, less commonly invoked safeguards including firewalls and network segmentation, and security audits and testing.

Multifactor Authentication Requirements

For MFA requirements, security regulations maintain a fairly consistent definition of what constitutes MFA, per NIST 800-53, but they vary in when they require it and whether they express any preference for certain types of MFA. Some examples of different provisions related to MFA are provided in Table 3.

Table 3: Provisions regarding multi-factor authentication in cybersecurity regulations, rules, and standards.

Source	Provision Regarding Multi-Factor Authentication
NIST 800-53 and FedRAMP	"Multi-factor authentication requires the use of two or more different factors to achieve authentication. The authentication factors are defined as follows: something you know (e.g., a personal identification number [PIN]), something you have (e.g., a physical authenticator such as a cryptographic private key), or something you are (e.g., a biometric)."
HIPAA Security Rule	"Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights"
FTC Safeguards Rule	"Implement multi-factor authentication for any individual accessing any information system … Multi-factor authentication means authentication through verification of at least two of the following types of authentication factors: (1) Knowledge factors, such as a password; (2) Possession factors, such as a token; or (3) Inherence factors, such as biometric characteristics."
Department of Education Privacy Technical Assistance Center	"Single-factor authentication may not be reasonable … for protecting access to highly sensitive information, including health records and information that could be used for identity theft and financial fraud, such as Social Security numbers (SSNs) and credit card numbers."
SEC Cybersecurity Risk Management Rules	"Advisers and funds may wish to consider multi-factor authentication methods that are not based solely on SMS-delivery (e.g., text message delivery) of authentication codes, because such methods may provide less security than other non-SMS based multi-factor authentication methods."
FFIEC Authentication and Access to Financial Institution Services and Systems	"When a financial institution management's risk assessment indicates that single-factor authentication with layered security is inadequate, MFA or controls of equivalent strength as part of layered security can more effectively mitigate risks. … The attributes, including usability, convenience, and strength, of various authentication factors can differ and each may exhibit different vulnerabilities which may be exploited. For example, certain MFA factors may be susceptible to MIM attacks, such as when a hacker intercepts a one-time security code sent to a customer."

NY DFS Cybersecurity Requirements for Financial Services Companies	"Covered Entities that have not filed a Notice of Exemption … must use MFA for remote access to all internal networks, including applications and systems, unless their CISOs have approved 'the use of reasonably equivalent or more secure access controls.' … Push-based MFA is more susceptible to human error than token-based MFA … Text message-based MFA is vulnerable to SIM-swapping."
FDA Cybersecurity in Medical Devices Guidance	"Use appropriate user authentication (e.g., multi-factor authentication to permit privileged, device access to system administrators, service technicians, or maintenance personnel, among others, as needed)"
NERC CIP Cyber Security Standards	"Require multi-factor authentication for all Interactive Remote Access sessions."
PCI DSS	"Implement two-factor authentication for all remote network access that originates from outside the network, by employees, administrators, and third parties including vendor access for support or maintenance. Examples of two-factor technologies include remote authentication and dial-in service (RADIUS) with tokens; terminal access controller access control system (TACACS) with tokens; or other technologies that facilitate two-factor authentication. Using one factor twice (e.g. using two separate passwords) is not considered two-factor authentication."
EPA Public Water Systems Cybersecurity Checklist	"While MFA may not be necessary for all systems, it does provide a higher degree of security and should be used wherever possible. Higher-risk access such as authenticating remote users or vendors should be done by MFA as much as possible."
TSA Security Directive Pipeline	"The owner/operator must… implement access control measures, including … multi-factor authentication, or other logical and physical security controls that supplement password authentication to provide risk mitigation commensurate to multi-factor authentication"
NIS2 Directive	"Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems … The measures … shall include at least the following: … the use of multi-factor authentication or continuous authentication solutions"

These examples range from HIPAA, which does not specifically invoke MFA in its security rule at all, to the NYDFS Cybersecurity Requirements for Financial Services Companies which mandate MFA or equivalent safeguards "for remote access to all internal networks." Many other regulations take an approach somewhere in between these two, requiring MFA be used for certain high-risk accounts and systems but not necessarily at all times. In its response to the ONCD RFI, the Mortgage Bankers Association (MBA) highlighted the challenges of trying to comply with this variety of different MFA requirements, especially for smaller companies. The MBA wrote:

> While the Safeguards Rule allows companies to use a risk-based approach to decide which systems require MFA, the recent version of the NY DFS Rule requires MFA for remote access to all third-party applications where personal information is accessible. This change effectively requires covered entities to switch their systems to comply with the NY DFS rule. The consequences of this fall most heavily on smaller firms. Companies that do not frequently interact with data security laws face the heaviest costs of compliance and must navigate these different laws while addressing the underlying security concern.[10]

The two primary areas of differentiation in MFA requirements are which systems or accounts the requirement applies to and whether it allows for all types of MFA or preferences certain categories of second factors. Broadly speaking, an MFA requirement may apply to all computer systems and accounts or a subset of particularly high-risk ones. The FTC Safeguards Rule, the NYDFS rule, and the European NIS2 Directive effectively take the former approach, while many of the other rules listed in Table 3 take the latter. There are also several different ways these guidelines define the subset of systems MFA must be applied to. For instance, the FFIEC guidance leaves it up to regulated entities to determined whether MFA is needed, according to their own risk assessments, while the EPA suggests that MFA be used "wherever possible," and the Department of Education offers still more roundabout guidance, warning that "Single-factor authentication may not be reasonable … for protecting access to highly sensitive information."

Still other regulatory approaches require either MFA or equivalent safeguards, such as the TSA Security Directive which requires pipeline owners and operators to use either MFA or "other logical and physical security controls that supplement password authentication to provide risk mitigation commensurate to multi-factor authentication." In its response to the ONCD RFI, Microsoft also highlighted the challenges of parsing subtle differences in the language used by regulators around when MFA should be used, pointing to the discrepancies between the TSA and EPA MFA requirements and noting that such differences are often not limited to just one security control. "This type of variance in language is often repeated across all requirements, which results in entities needing to analyze and interpret what is required to comply with different regulations," Microsoft noted.[11]

One final opportunity for harmonization across the different MFA requirements centers on whether or not they specify which types of MFA are preferable or most secure. Many of the rules listed in Table 3 adhere to the NIST 800-63 definition of MFA as two of the following three types of factors: "something you know, something you have, or something you are" and do not specify which of these factors should be used. However, a few do note some preferred implementations. For instance, the SEC rules urge regulated entities "to consider multi-factor authentication methods that are not based solely on SMS-delivery (e.g., text message delivery) of authentication codes, because such methods may provide less security than other non-SMS based multi-factor authentication methods." The FFIEC Authentication and Access guidance also cautions against the use of one-time codes as a second factor, warning that "certain MFA factors may be susceptible to MIM attacks, such as when a hacker intercepts a one-time security code sent to a

[10] Mortgage Bankers Association, RE: Request for Information on Cyber Regulatory Harmonization [RIN: 0301-AA00], October 31, 2023. Available from https://www.regulations.gov/comment/ONCD-2023-0001-0029.

[11] Microsoft, "Re: Microsoft Comments on ONCD's Cyber Regulatory Harmonization RFI, Docket ID: ONCD-2023-0001," October 31, 2023. Available from https://www.regulations.gov/comment/ONCD-2023-0001-0080.

customer." Meanwhile, NYDFS advises that "Push-based MFA is more susceptible to human error than token-based MFA" and "Text message-based MFA is vulnerable to SIM-swapping." This suggests a variety of ways that regulators can—and do—try to encourage regulated entities not to use specific types of MFA (such as SMS-based codes, push-based second factors, and one-time security codes), as well as to encourage those same entities to use other more secure forms of MFA, such as token-based MFA.

However, there is not always clear consensus around the appropriate implementation of MFA for different contexts. For instance, in their response to the ONCD RFI, researchers from Georgia Tech noted that many cybersecurity regulations fall short of advising regulated entities about the most effective forms of MFA, leading to many regulated entities providing only insecure MFA implementations, such as one-time codes sent via text message.[12] By contrast, in their comments in response to the RFI, Deloitte advocated for more "flexibility" in defining preferred MFA implementations, noting that, "although Short Message Service (SMS)-based multi-factor authentication (MFA) is deprecated in recent NIST publications, it may still make sense for telecommunication providers who directly own the customer relationship."[13] Harmonizing MFA requirements will require not just consensus around when MFA should be used and which systems it should apply to, but also which types of MFA are appropriate and adequately secure for different contexts and systems.

Opportunities for Harmonizing Multifactor Authentication Requirements

Two key questions around harmonizing multifactor authentication requirements emerge from this review of existing cybersecurity regulations: (1) Must MFA be applied to all systems and accounts? And (2) Are all forms of MFA permitted or are some not considered sufficiently secure? In this section, we consider briefly the potential answers to each of these questions as well as the advantages and disadvantages of each option, and the rationale for allowing some variation across different sectors' answers.

Harmonization Question #4: Must MFA be applied to all systems and accounts?

- Option #4.1: MFA is required for all remote access
    - Advantages: Clear guidance, high level of authentication security for all systems.
    - Disadvantages: May be difficult to implement for legacy systems, third-party vendors may not have access to MFA.
- Option #4.2: MFA is required only for high-risk systems
    - Advantages: Allows for risk-based approach that reduces friction for systems where authentication may be lower stakes.
    - Disadvantages: Subjective assessments of the risk level of different systems; potential for a low-risk system to be used to compromise a higher risk one.
- Option #4.3: MFA may be replaced with commensurate security measures
    - Advantages: Flexibility for systems that do not work well with MFA (legacy systems, multi-user systems, etc.).

[12] McKay Moore and Annie Antón, October 31, 2023. Available from https://www.regulations.gov/comment/ONCD-2023-0001-0059.

[13] Deloitte, "RFI No. ONCD-2023-0001 Opportunities for and Obstacles to Harmonizing Cybersecurity Regulations," October 20, 2023. Available from https://www.regulations.gov/comment/ONCD-2023-0001-0011.

    - Disadvantages: Unclear which controls are commensurate with MFA, provides loophole for MFA requirement.
- Rationale for variation across industry sectors: Industry sectors with different risk profiles may have different tolerance levels for less secure authentication methods or be more reliant on legacy systems that may not be compatible with MFA.
- Recommended baseline definition: Option #4.2 (with opportunity to extend it by adding options 4.1 or 4.3 as needed, with relevant justification).

Harmonization Question #5: Are all forms of MFA permitted or are some not considered sufficiently secure?

- Option #5.1: Allow all forms of MFA that involve the use of two different factors
    - Advantages: Flexible for different organizations and MFA implementations.
    - Disadvantages: Allows for use of MFA implementations with known vulnerabilities.
- Option #5.2: Discourage or disallow use of SMS-based MFA
    - Advantages: Deprecates MFA system known to be vulnerable to SIM swapping.
    - Disadvantages: May make MFA implementation more difficult for some users.
- Option #5.3: Discourage or disallow use of push-based MFA in favor of token-based MFA.
    - Advantages: Deprecates MFA system known to be susceptible to people accidentally approving login requests.
    - Disadvantages: Makes MFA more time-intensive for users, adding friction to login process.
- Option #5.4: Discourage or disallow use of one-time code-based MFA systems.
    - Advantages: Deprecates MFA system known to be susceptible to man-in-the-middle attacks.
    - Disadvantages: More difficult for users in some cases and more expensive to implement if using physical tokens.
- Rationale for variation across industry sectors: Different organizations may have different levels of tolerance for more and less secure MFA implementations, and may have more or less control over different second factors (e.g., telcos and SMS messages).
- Recommended baseline definition: Option #5.2 (with opportunity to extend or roll it back by exchanging for option 5.1 or adding options 5.3 or 5.4 as needed, with relevant justification).

Encryption Requirements

Another commonly used security control that is dealt with inconsistently across different cybersecurity regulations is encryption. Some examples of different regulatory and policy encryption requirements are provided in Table 4.

Table 4: Provisions regarding encryption in cybersecurity regulations, rules, and standards.

Source	Provision Regarding Encryption

FIPS 140-2 and FedRAMP	“Security control SC-13 requires that FIPS 140-validated or NSA-approved cryptographic modules (CMs) are used … The Cryptographic Module Validation Program (CMVP) is a joint effort between the National Institute of Standards and Technology under the Department of Commerce and the Canadian Centre for Cyber Security… Cryptographic and Security Testing Laboratories (CSTL) verify each module meets a set of testable cryptographic and security requirements, with each CSTL submission reviewed and validated by CMVP.”
HIPAA Security Rule	“Implement a mechanism to encrypt and decrypt electronic protected health information.”
FTC Safeguards Rule	“Protect by encryption all customer information held or transmitted by you both in transit over external networks and at rest. To the extent you determine that encryption of customer information, either in transit over external networks or at rest, is infeasible, you may instead secure such customer information using effective alternative compensating controls”
NERC CIP Cyber Security Standards	“For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System. … Encryption is needed when there is a risk of unauthorized interception of transmissions on the communications link.”
NY DFS	“Each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest.”
FDA Cybersecurity in Medical Devices Guidance	“Manufacturers should ensure support for the confidentiality of any/all data whose disclosure could lead to patient harm (e.g., through the unauthorized use of otherwise valid credentials, lack of encryption). Loss of confidentiality of credentials could be used by a threat-actor to effect multi-patient harm. Lack of encryption to protect sensitive information and or data at rest and in transit can expose this information to misuse that can lead to patient harm.”
PCI DSS	“Use strong cryptography and security protocols such as TLS, SSH or IPSec to safeguard sensitive cardholder data during transmission over open, public networks … Strong cryptography is based on industry-tested and accepted algorithms along with key lengths that provide a minimum of 112-bits of effective key strength and proper key-management practices.”
EPA Public Water Systems Cybersecurity Checklist	“When sending information and data, use Transport Layer Security (TLS) or Secure Socket Layer (SSL) encryption standards.”
NIS2 Directive	“Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems … The measures … shall include at least the following: … policies and procedures regarding the use of cryptography and, where appropriate, encryption”

As with MFA, the crucial points of divergence in these regulations relate to when and where encryption should be applied and what type of encryption should be used. For instance, several regulations specify that data should be encrypted either in motion (PCI DSS, EPA), at rest, or both (NY DFS, FTC Safeguards, FDA). Related to the different definitions of personal information discussed in the previous section, these regulations also designate different categories of data that must be protected with encryption, ranging from "sensitive cardholder data" (PCI DSS) and "customer information" (FTC Safeguards) to "electronic protected health information" (HIPAA) and "nonpublic information" (NY DFS). Taking yet another approach, the FDA guidance for medical devices designates a need to encrypt "any/all data whose disclosure could lead to patient harm," choosing to focus on the potential impacts of a breach rather than the specific types of data that should be protected. These discrepancies point to how interrelated issues of regulatory harmonization are in this space—harmonizing encryption requirements will also entail some degree of harmonizing definitions of personal data, even if different sector-specific regulations continue to focus on different categories of data.

Another opportunity for harmonization across encryption requirements relates to the specific encryption algorithms and tools that regulated entities must use to protect data. Not all regulations or rules specify specific technical standards, but a few do. Some, such as the EPA and PCI DSS cite specific widely used security protocols, such as TLS, SSL, and SSH, while the PCI DSS also call for the use of "industry-tested and accepted algorithms" with a minimum key length of 112 bits. FedRAMP does not specify particular encryption algorithms or key lengths, but instead requires companies to use cryptographic modules that have been validated by FIPS 140 or approved by the NSA through the Cryptographic Module Validation Program (CMVP) jointly run by NIST and the Canadian Centre for Cyber Security. This approach has the advantage of allowing for regular updates as new cryptographic modules are developed, but also places a potentially larger compliance burden on firms that must seek approval from the CMVP in order to use new cryptographic methods.

Overall, there appear to be significant opportunities to harmonize cybersecurity regulations with regards to what types of data must be encrypted and when, as well as how those encryption protections ought to be implemented. While there may be some differences across industry sectors in terms of the relevant types of data, it would seem plausible that a similar set of technical standards would apply across different use cases to provide adequate protection from disclosure or unauthorized access.

Opportunities for Harmonizing Encryption Requirements

Two key questions around harmonizing encryption requirements emerge from this review of existing cybersecurity regulations: (1) Should encryption be applied to all personal/sensitive data in motion and at rest? And (2) Which types of encryption are considered adequate for data protection? In this section, we consider briefly the potential answers to each of these questions as well as the advantages and disadvantages of each option, and the rationale for allowing some variation across different sectors' answers.

Harmonization Question #6: Should encryption be applied to all personal/sensitive data in motion and at rest?

- Option #6.1: Encryption required for all sensitive data in motion and at rest

    - Advantages: Clear guidance; offers more security for data at all times.
    - Disadvantages: May inhibit organizations' ability to analyze and use their data while it is at rest.
- Option #6.2: Encryption required for all sensitive information in motion
    - Advantages: Allows for organizations to perform more analysis of data while it is being stored and use it for other purposes (e.g., model training).
    - Disadvantages: May make it more difficult to analyze network traffic for anomalies and threats; allows for unencrypted data at rest that may be compromised.
- Option #6.3: Encryption not required for sensitive data
    - Advantages: Easy for organizations to use their data and monitor their network traffic.
    - Disadvantages: Compromised data will be available to intruders in cleartext.
- Rationale for variation across industry sectors: Industry sectors may have different needs when it comes to being able to access and use unencrypted data and monitor network traffic.
- Recommended baseline definition: Option #6.2 (with opportunity to extend it by adding 6.1 or roll it back by replacing with 6.3 as needed, with relevant justification).

Harmonization Question #7: Which types of encryption are considered adequate for data protection?

- Option #7.1: Allow organizations to choose their own encryption tools and algorithms
    - Advantages: Flexibility enables organizations to take a risk-based approach and tailor encryption to their purposes.
    - Disadvantages: May mean that some organizations use weak encryption that can be broken by intruders.
- Option #7.2: Mandate specific encryption algorithms and protocols or key lengths
    - Advantages: Offers clarity to organizations, especially small businesses without in-house technical expertise.
    - Disadvantages: May be difficult to keep approved algorithms up-to-date, and may limit diversity of encryption tools used.
- Option #7.3: Require encryption tools and algorithms to be approved by a technical authority
    - Advantages: Clear guidance; allows for organizations to choose their own encryption tools while still ensuring those tools are secure.
    - Disadvantages: May be onerous for both regulated entities and regulators to go through/oversee the approval process.
- Rationale for variation across industry sectors: Different organizations may require different degrees of protection for their data and have differing amounts of resources to invest in approval processes or encryption tools and services.
- Recommended baseline definition: Option #7.2 (with opportunity to extend it by adding 7.3 or roll it back by replacing with 7.1 as needed, with relevant justification).

Network Segmentation & Firewall Requirements

While MFA and encryption are two of the most widely cited security controls in cybersecurity regulations, rules and standards also invoke a variety of other measures, though often with less specificity. For instance, several rules and regulations reference a need for firewalls and network segmentation. PCI DSS, for example, requires that companies “build firewall and router configurations that restrict all traffic, inbound and outbound, from ‘untrusted’ networks (including wireless) and hosts, and specifically deny all other traffic except for protocols necessary for the cardholder data environment” and that the companies “prohibit direct public access between the Internet and any system component in the cardholder data environment.”

The EPA recommendations for public water systems, by contrast, instruct utilities to “only allow connections to the OT network from the IT network via approved assets and other approved means” and by default to “deny all connections to the OT network from the IT network unless explicitly allowed (by IP address and port) for specific system functionality.” The TSA pipeline security directive imposes a similar requirement on pipeline companies to “implement network segmentation policies and controls designed to prevent operational disruption to the Operational Technology system if the Information Technology system is compromised or vice versa.” TSA further prohibits “Operational Technology system services from traversing the Information Technology system, unless the content of the Operational Technology system is encrypted while in transit,” thereby highlighting the overlap between segmentation and encryption policies and the need to harmonize them in tandem.

These different approaches to segmentation also suggest a few different models for regulation: prohibiting access between the public internet and a protected system as in PCI DSS, or connections between OT and IT networks (EPA), or allowing such connections only in the event that the OT data is encrypted (TSA). While different approaches may make more sense for different network contexts, it may also be possible to align these requirements more closely given that they all share the same high-level goal of containing the spread of any compromise in one part of the network.

Audit, Testing & Assessment Requirements

Like network segmentation, security audits, assessment, and testing practices are also invoked in several regulations and rules in a variety of different ways. For instance, the TSA directive requires pipeline companies to conduct annual exercises to test security measures and to “ensure that at least 30 percent of policies, procedures, measures, and capabilities in the TSA-approved Cybersecurity Implementation Plan are assessed each year, with 100 percent assessed over any three-year period.” PCI DSS, the FTC Safeguards Rule, and the NYDFS Cybersecurity Requirements mandate annual penetration testing, with the PCI DSS also specifying that those tests be used to assess that network segmentation measures are operational and effective, again highlighting the interrelatedness of different security requirements. Here again, there may be opportunities to harmonize both the timeline of penetration testing, vulnerability assessments, and security exercises as well as who must perform them (self-certification versus external third parties) and which security controls and measures they are required to assess (all versus a percentage each year).

In some cases, standardization of these requirements may help alleviate the burden of complying with onerous auditing or testing expectations. For instance, in its response to the ONCD RFI, Red Alert Labs noted:

> electric utilities with medium and high impact assets are required to self-certify their compliance with all the CIP requirements annually, but they are subject to onsite audits once every 3-6 years. However, because of the number of CIP requirements and the fact that a huge amount of compliance evidence is required at audits, the onsite audits almost never address all the requirements (the entity will not usually know until a few months before the audit which requirements will be covered, so they have to continually gather evidence for all of them).[14]

In other words, the number of cybersecurity requirements undermines the thoroughness of the onsite audits, because they cannot address every requirement. More generally, a lack of standardization across baseline security requirements in regulations compounds the challenges of conducting consistent audits for compliance purposes.

Similar opportunities for harmonization apply to provisions regarding the development of incident response plans, logging policies, patching requirements, and continuous monitoring, though in many cases these requirements are sufficiently vague to allow for considerable flexibility across regulations. This vagueness does not always serve regulated entities well, however, since it can complicate the auditing process. As SAFE Credit Union points out in its response to the RFI, “Auditors apply findings based on these vague requirements; however, most of the time each auditor is applying their personal interpretation of the requirements to substantiate the finding.”[15] This is another example of how harmonizing some components of cybersecurity regulations (such as security control baseline requirements) can enable harmonization of other provisions, such as audit requirements. In the absence of harmonized requirements, it may still be possible to eliminate some auditing redundancies by establishing agreements among different government entities that they will accept the cybersecurity assessments and audits that guarantee compliance with other agencies’ requirements. However, these agreements will probably be easier to achieve in areas where the baseline requirements are similar, if not the same, suggesting that it may be easier to harmonize audit and assessment standards following the alignment of baseline security standards.

Opportunities for Harmonization: Reporting Requirements

In addition to requirements around cybersecurity measures and policies, cybersecurity regulations also diverge significantly around reporting requirements linked to security incidents and breaches. The ONCD RFI explicitly excluded this from the scope of their inquiry, telling respondents on the grounds that “such requirements are being analyzed through a separate effort led by the Cyber Incident Reporting Council established by the Secretary of Homeland

[14] Red Alert Labs, “Red Alert Labs: Responses to ‘Questions for Respondents’ for ONCD RFI on Cybersecurity Regulatory Harmonization,” Sept. 14, 2023. Available from https://www.regulations.gov/comment/ONCD-2023-0001-0005.

[15] SAFE Credit Union, “Re: Docket No.: ONCD-2023-0001 or RIN 0301-AA00 Opportunities For and Obstacles To Harmonizing Cybersecurity Regulations,” October 24, 2023. Available from https://www.regulations.gov/comment/ONCD-2023-0001-0016.

Security as required by [CIRCIA].” However, it is still worth considering three different elements of cybersecurity reporting regimes that might benefit from harmonization: the timeline required for reporting, what information must be reported, and whom it must be reported to.

Reporting Timelines

One of the major sources of variance across cybersecurity reporting guidelines and requirements is the timeframe in which incidents must be reported. Despite ONCD’s injunction not to submit comments to its RFI on reporting regulations, several respondents still raised these discrepancies, including Cooperative Exchange which submitted a chart mapping the different timelines of state breach notification laws, which range from 90 days to 1 day, with the largest number of states that specified a deadline setting it at 45 days and another 32 states not specifying any precise timeline other than that reports must be made “without unreasonable delay.”[16] Other organizations also highlighted discrepancies in reporting timelines, with the American Bankers Association pointing out that while CIRCIA mandates reporting of incidents within 72 hours of discovery and reporting of ransoms within 24 hours of payment, other entities such as the CFTC System Safeguards Rule merely require that reporting be done “promptly.”[17] The National Defense Industry Association (NDIA) offered similar critiques in its comments, noting that incident reporting deadline timeframes range from “as little as 8 hours in the recent FAR Case 2021-017 to a more frequent, but sometimes unworkable, 24 to 72 hours.”[18]

Notably, as reporting requirements have become increasingly common, regulations and rules continue to impose new, shorter timelines on reporting. For instance, TSA updated its requirements for high-risk rail providers in 2021 to impose a 24-hour time limit on reporting cybersecurity incidents. In 2024, the US Coast Guard proposed similar changes to its Cybersecurity in the Marine Transportation System rules, requiring that cybersecurity incidents be reported no more than 24 hours after their discovery or occurrence. The SEC, meanwhile, has proposed a deadline of four days for businesses to file paperwork and Form 8-K disclosing material cybersecurity incidents. The Association of American Railroads notes in its response to the RFI, “These competing time frames and definitions can create unnecessary confusion and burden on those seeking to comply.”[19]

While it may make sense to have certain critical infrastructure incidents reported more rapidly than other, lower risk incidents, the variation in reporting timelines would seem to be an ideal opportunity for harmonization, especially since it is not clear how much the differences between 24-hour, 72-hour, and 96-hour deadlines actually matter in terms of regulators’ ability to respond. In its 2023 report on “Harmonization of Cyber Incident Reporting to the Federal Government,” the Department of Homeland Security recommended that reporting timelines shorter than 72 hours should be limited to “Agencies with requirements related to national and economic security and safety … especially where incidents may affect [national critical functions] or the

[16] Cooperative Exchange, “RE: RFI, RIN 0301-AA00,” October 31, 2023. Available from https://www.regulations.gov/comment/ONCD-2023-0001-0075.

[17] American Bankers Association, October 31, 2023. Available from https://www.regulations.gov/comment/ONCD-2023-0001-0069.

[18] NDIA, October 31, 2023. Available from https://www.regulations.gov/comment/ONCD-2023-0001-0085.

[19] Association of American Railroads, October 31, 2023. Available from https://www.regulations.gov/comment/ONCD-2023-0001-0023.

delivery of vital goods and/or services to customers or the public."[20] This would suggest a fairly high threshold for incidents that would require a reporting timeline under 72 hours and would, accordingly, correspond to a fairly narrow definition of incidents with particularly significant immediate impacts.

Reporting Incident Information

A second set of opportunities for harmonizing cybersecurity reporting regulations relates to the question of what regulated entities are supposed to report about these incidents. Many of the state data breach notification laws provide fairly vague guidelines, requiring in some cases just the disclosure of what information is believed to have been stolen, when the breach occurred, and who victims can contact for further inquiries or support. More recent reporting regulations, however, often impose much broader requirements on the information that must be reported. For instance, the SEC's amendments to Form 8-K would require disclosure of:

- When the incident was discovered and whether it is ongoing;
- A brief description of the nature and scope of the incident;
- Whether any data were stolen, altered, accessed, or used for any other unauthorized purpose;
- The effect of the incident on the registrant's operations; and
- Whether the registrant has remediated or is currently remediating the incident.

This type of more in-depth reporting offers more potential analysis of threat trends and countermeasure effectiveness, but also adds to the complexity and time required to be able to issue thorough reports. Ironically, many of these more recent regulations requiring more in-depth reports also have shorter deadlines for reporting, making it more difficult for organizations to conduct thorough investigations and identify the necessary information to issue a complete report by the deadline.

In a similarly vein, CIRCIA reporting requirements include a "description of the covered cyber incident," including the name and a description of the impacted systems, networks, and/ or devices, to include technical details and physical locations of the impacted systems, networks, and/or devices, and whether the incident involved any unauthorized access, whether there were any informational impacts, or whether any information was compromised, as well as the date the covered cyber incident was detected, the date the covered cyber incident began (if known), and the date the covered cyber incident was fully mitigated and resolved. Additional categories of information to be reported under CIRCIA include "a description of the vulnerabilities exploited and security defenses in place, as well as the tactics, techniques, and procedures used to perpetrate the covered cyber incident," as well as "any identifying or contact information related to each actor reasonably believed to be responsible for such cyber incident." Additionally, CISA has proposed including "a small number of questions regarding the mitigation and response activities a covered entity is taking or has taken in response to a covered cyber incident" as part of the CIRCIA Incident Reporting Form as well.

[20] Department of Homeland Security Office of Strategy, Policy and Plans. "Harmonization of Cyber Incident Reporting to the Federal Government." September 19, 2023. Available from https://www.dhs.gov/sites/default/files/2023-09/DHS%20Congressional%20Report%20-%20Harmonization%20of%20Cyber%20Incident%20Reporting%20to%20the%20Federal%20Government.pdf.

These reporting details would again suggest an opportunity for harmonization and aligning the information compromised entities must gather for different regulators. In addition to lessening the burden on regulated entities, a unified reporting regime would also potentially enable better, more thorough analysis of incidents on the government's part if incidents were all reported using the same information fields and format.

Reporting Authorities

Unsurprisingly, different reporting regulations typically require entities to report cybersecurity incidents to different authorities. In the case of state breach notification laws, these reports are typically made either to state attorneys general or the affected individuals, in the case of federal rules and regulations, the reports are usually made to the regulating agency (TSA, CISA, EPA, etc.) There may be good reasons to report sector-specific incidents to the relevant regulatory agency, but it is worth noting that harmonization of reporting regimes will almost certainly require some greater alignment of whom reports are made to, even if they can then be shared with the relevant authority.

As with report information, centralizing the reporting infrastructure to a single entity that is then responsible for distributing those reports to the relevant agencies could enable more thorough analysis of aggregated incident reports, especially if they were all submitted according to a uniform format. Here, again, multiple harmonization efforts will have to be undertaken simultaneously, since harmonization of whom entities must report to will be ineffective at reducing compliance burdens unless it is also coupled with harmonization of reporting timelines and report contents.

Opportunities for Harmonizing Reporting Requirements

Three key questions around harmonizing reporting requirements emerge from this review of existing cybersecurity regulations: (1) How long do organizations have to report a security incident? (2) What information do organizations have to report about an incident? And (3) To whom should incidents be reported? In this section, we consider briefly the potential answers to each of these questions as well as the advantages and disadvantages of each option, and the rationale for allowing some variation across different sectors' answers.

Harmonization Question #8: How long do organizations have to report a security incident?

- Option #8.1: 24 hours
    - Advantages: Opportunity for very rapid response on the part of regulators.
    - Disadvantages: Very little opportunity to investigate incident prior to reporting.
- Option #8.2: 72 hours
    - Advantages: Allows for some initial investigation while still enabling relatively rapid response.
    - Disadvantages: No time for an in-depth investigation or root cause analysis prior to reporting.
- Option #8.3: 10+ days
    - Advantages: Allows for more in-depth investigation of incident prior to reporting.
    - Disadvantages: Missed opportunity for immediate remediation or response.

- Rationale for variation across industry sectors: Different sectors may have differing abilities to wait for reports depending on their risk tolerance and the potential impacts of an incident.
- Recommended baseline definition: Option #8.2 (with opportunity to extend or shorten the reporting timeline as needed, with appropriate justification).

Harmonization Question #9: What information do organizations have to report about an incident?

- Option #9.1: Brief summary of what occurred and what information or systems were affected
  - Advantages: Relatively small burden for organizations, easy to accomplish in short amount of time.
  - Disadvantages: Very difficult to learn from incidents when so little is known about how and why they occurred.
- Option #9.2: Summary description of incident, impacts, and remediation efforts
  - Advantages: Offers more detail about an incident's impacts and remediation.
  - Disadvantages: May require more time to compile information about impacts.
- Option #9.3: Detailed description of incident, impacts, remediation efforts, vulnerabilities, countermeasures, and responsible perpetrators
  - Advantages: Offers much more information for long-term analysis of threat landscape, security control effectiveness, and attribution.
  - Disadvantages: Requires more time to conduct a thorough investigation, may necessitate a multi-step reporting process over a longer timeline.
- Rationale for variation across industry sectors: Different types of incidents may require more or less after-the-fact analysis to understand how they occurred and what can be learned from them, depending on how sophisticated they are, how much effort the perpetrators have put into obfuscating their actions, and how long it takes victims to recover.
- Recommended baseline definition: Option #9.2 (with opportunity to expand to 9.3 or roll back to 9.1 as needed, with proper justification).

Harmonization Question #10: To whom should incidents be reported?

- Option #10.1: Centralized reporting authority
  - Advantages: Allows for more aggregate analysis of incident data; creates simpler, more streamlined reporting structure for organizations.
  - Disadvantages: May mean that the relevant authorities are not promptly notified of incidents in some cases.
- Option #10.2: Individual regulators and agencies
  - Advantages: Enables prompt notification of the relevant authorities.
  - Disadvantages: May require organizations to duplicate their reporting efforts.
- Option #10.3: Public audience
  - Advantages: Enables greater public awareness of threat landscape and risks.
  - Disadvantages: May discourage organizations from sharing more information in these reports.
- Rationale for variation across industry sectors: Certain types of incidents—such as those that affect individuals—may warrant public announcements to enable consumer

protection efforts, while others may only require the attention and awareness of relevant sector regulators and industry partners

- Recommended baseline definition: Option #10.1 (with opportunity to add 10.2 or 10.3 as needed, with proper justification).

A Roadmap for Moving Forward with Regulatory Harmonization

This report has reviewed several areas of divergence across different cybersecurity regulations, rules, and standards in order to identify opportunities for harmonization. These opportunities, as well as the advantages and disadvantages of each potential approach, are summarized in the ten harmonization questions discussed in the previous sections. While the questions identified in this report and the associated options for harmonization are certainly not the only ones that need to be answered for moving forward with harmonizing the cybersecurity regulatory landscape, they offer a good starting point for tackling some of the most urgent and burdensome discrepancies in existing cybersecurity regulation identified by organizations in their responses to the ONCD RFI.

Harmonization need not mean that every regulation and industry sector impose exactly the same requirements and uses exactly the same definitions when it comes to cybersecurity. However, ideally any decisions to diverge from each other would be deliberate, considered, and justified according to the risk profile or particular nature of the regulation in question. By laying out the different approaches that have been taken in existing regulations, rules, and standards, regulators can begin to consider whether the differences across these sources are necessary and important for cybersecurity purposes. In some cases, it seems possible that these discrepancies are instead the result of different regulatory agencies drawing on their respective decision-making processes and resources to craft their own language and approaches.

By studying the approaches taken by their peers, regulators may therefore encounter opportunities to harmonize their regulations and also learn from the experience of other sectors and agencies. This aligns with the recommendations offered by the President's National Security Telecommunications Advisory Committee (NSTAC) in their 2023 report, urging the creation of an Office of Cybersecurity Regulatory Harmonization within CISA to help establish consensus standards for cybersecurity regulations. Once such a framework had been established, NSTAC suggested, government agencies issuing federal cybersecurity requirements would then have to "align them to existing consensus standards or provide justification for why requirements diverge from existing consensus standards."[21]

One crucial trade-off that regulators will be faced with in trying to harmonize cybersecurity regulations is the balance between specific rules, which offer clear guidance to regulated entities, and vaguer more flexible cybersecurity rules and definitions. In many ways, these more flexible rules are better suited to harmonization because different types of organizations and regulators can adapt them to different contexts, but they also offer less clear-cut requirements for what

[21] National Security Telecommunications Advisory Committee. "Strategy for Increasing Trust in the Information and Communications Technology and Services Ecosystem." February 21, 2023. Available from https://www.cisa.gov/sites/default/files/2023-04/NSTAC_Strategy_for_Increasing_Trust_Report_%282-21-23%29_508_0.pdf.

organizations must do to protect their data and networks. This tension is already apparent in many of the RFI responses that call on the U.S. government to harmonize cybersecurity regulations around the NIST Cybersecurity Framework (CSF).

The NIST CSF offers no specific definitions, security control requirements, or reporting guideline. Rather, it offers organizations a step-by-step approach to identifying their cybersecurity risks and then maps those risks onto existing catalogs of security controls. As such, it is entirely non-prescriptive and provides regulated entities with maximal freedom to design their own approaches to cybersecurity in accordance with their own risk assessments. It's not surprising, given the high-level non-prescriptive approach it takes, that the NIST CSF is an appealing reference point for harmonization to many organizations. But it can also be viewed as a bit of a cautionary tale—a framework so broad that many different government agencies have either deemed it inadequate as cybersecurity guidance for the organizations in their sectors, or interpreted it and developed more specific guidance on top of its broad framework in a variety of diverging directions, enabling the patchwork of different overlapping rules we have today. For a baseline framework to provide consistent, harmonized regulations across industry sectors, it may need to be more specific or prescriptive than the CSF to satisfy agencies' concerns about organizations meeting minimum security standards.

Notably, deciding to use the CSF across different cybersecurity regulations would not resolve any of the areas and opportunities for harmonization described above. Rather, it would empower organizations to each take their own approaches to securing their data and networks so long as they used the process laid out in the CSF. This would seem unlikely to satisfy the regulators who have taken much more detailed, concrete approaches to regulating cybersecurity, including TSA, CISA, the FTC and the SEC. So, while approaching regulatory harmonization from this vantage point of allowing organizations maximal flexibility may seem appealing, it could also backfire and lead to the proliferation of yet more different regulations if regulators discover that a flexible approach leads to some organizations implementing inadequate security controls, especially in critical infrastructure sectors.

As Verizon points out in its response to the RFI:

> Presumably, the concerns underlying policies that layer specific "baseline" cybersecurity controls over the overarching CSF plan requirements is the fact that a company's mere use of the CSF does not, on its own, ensure any specific level of cybersecurity maturity. Indeed, while some companies may use the CSF to drive sophisticated, comprehensive cybersecurity outcomes, others' use of the CSF may be nascent and minimalistic. ONCD and the rest of the federal government should therefore explore ways to promote interagency collaboration to ensure minimum levels of CSF implementation by communications sector members.[22]

As a possible solution, Verizon suggests that the CSF could be required to be implemented at a particular implementation tier, but even that would leave organizations considerable leeway to tailor their own cybersecurity programs. That's not necessarily a bad thing—in some cases, as discussed above, there are good reasons for different sectors and organizations to tailor their approaches to cybersecurity protections and remediation efforts. But cybersecurity regulations typically are not designed to target the organizations that are already heavily investing in

[22] Verizon, October 31, 2023. Available from https://www.regulations.gov/comment/ONCD-2023-0001-0051.

security, they are often meant to drive adoption of security practices and controls among lagging organizations.

There is some advantage to considering the role of specificity in harmonization efforts given that such efforts are more likely to endure and resist proliferation of new regulations if they are viewed by regulators as yielding good security outcomes for even those lagging organizations. Harmonization efforts aimed at eliminating specific requirements may lessen the compliance burdens on regulated entities in the short term, but they may ultimately backfire in the long-term if regulators decide that the harmonized regulations are insufficiently stringent and warrant the introduction of new, additional requirements.

One possibility would be to use the widespread regard for the CSF as a starting point for building a more specific baseline framework on top of it. This could be done by, for instance, selecting a set of specific security controls from the different tiers in the CSF to serve as a consensus guideline for minimum requirements. Despite being more prescriptive than the CSF, such a framework might be able to capitalize on some of industry's familiarity and comfort with the CSF to impose a more specific set of requirements under a broad framework that many organizations are already accustomed to using. This could provide a shared starting point for government agencies proposing sector-specific cybersecurity requirements as well, since they could begin by selecting a particular tier of baseline controls and then add to those controls as needed under the categories and functions defined by the CSF, without imposing an entirely new set of definitions or requirements. By starting from a flexible framework like the CSF that has widespread acceptance in industry, it may be possible to work towards a more concrete, specific baseline framework that still feels familiar and manageable to both regulators and regulated entities, alike.

Acknowledgments

Microsoft provided support for this project, and Jason Healey provided invaluable feedback on an earlier draft.