ITI Promoting Innovation Worldwide

Written Testimony of
John S. Miller
Senior Vice President of Policy and General Counsel
Information Technology Industry Council (ITI)

Before the
Committee on Homeland Security
Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation

Stakeholder Perspectives on the Cyber Incident Reporting for Critical Infrastructure Act of 2021

September 1, 2021

Chairwoman Clarke, Ranking Member Garbarino, and Distinguished Members of the Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation of the House Committee on Homeland Security, thank you for the opportunity to testify today. My name is John Miller, Senior Vice President of Policy and General Counsel at the Information Technology Industry Council (ITI).[1] I lead ITI's Trust, Data, and Technology team, including our work on cybersecurity policy globally, and I have deep experience working on public-private security initiatives in the United States, including currently serving as Co-chair of the Cybersecurity and Infrastructure Security Agency (CISA)-sponsored Information and Communications Technology Supply Chain Risk Management Task Force (ICT SCRM Task Force), and as Vice Chair of the Information Technology Sector Coordinating Council (ITSCC), the principal IT sector partner to CISA on critical infrastructure protection and cybersecurity policy. I am honored to provide ITI's perspective on the important topic of cyber incident reporting and the legislation the Subcommittee is considering today.

ITI represents the world's leading information and communications and technology (ICT) companies. We promote innovation worldwide, serving as the ICT industry's premier advocate and thought leader in the United States and around the globe. ITI's membership comprises leading innovative companies from all corners of the technology sector, including hardware, software, digital services, semiconductor, network equipment, cybersecurity and other internet and technology-enabled companies that rely on ICT to evolve their businesses. Cybersecurity is rightly a priority issue for governments and our industry, and we share the common goals of improving cybersecurity, protecting the privacy of individuals' data, and maintaining strong intellectual property protections. Further, our members service customers across all levels of government and the full range of global industry sectors, such as financial services, healthcare, and energy. We thus acutely understand the importance of cybersecurity as not only a global business imperative for companies and customers alike, but as critical to our collective security. As a result, our industry has devoted significant resources, including expertise, initiative, and

[1] See ITI membership list at: https://www.itic.org/about/membership/iti-members.

Global Headquarters
700 K Street NW, Suite 600
Washington, D.C. 20001, USA
+1 202-737-8888

Europe Office
Rue de la Loi 227
Brussels - 1040, Belgium
+32 (0)2-321-10-90

info@itic.org
www.itic.org
@iti_techtweets

investment in cybersecurity efforts to create a more secure and resilient Internet ecosystem.

The SolarWinds compromise and the latest wave of damaging ransomware attacks, along with other recent cyberattacks, serve as an important reminder that the cyber threat landscape is constantly evolving and that we need innovative new policy ideas to help confront the emergence of new threats. We have seen policymakers increasingly consider incident reporting as a potentially appropriate tool to improve government's ability to leverage its resources towards not only helping victim organizations recover from incidents, but ideally to help protect others from similar threats or vulnerabilities. If narrowly scoped and carefully crafted, we believe that an incident reporting regime can help improve the nation's digital resilience and security.

We commend the Subcommittee for its leadership on this issue and its commitment to developing an effective and efficient cybersecurity incident reporting regime. As a general matter, we appreciate that the *Cyber Incident Reporting for Critical Infrastructure Act of 2021* (hereafter "the Act") leaves many of the details to be worked out through a rulemaking process in which CISA solicits feedback from stakeholders, as opposed to laying out stringent requirements in statute.

Just last month ITI published our *Policy Principles for Cyber Incident Reporting in the United States* (hereafter "*Policy Principles"*) to help inform ongoing efforts domestically, which is attached as an Appendix to my testimony (see Appendix A). We make ten recommendations to policymakers in the *Policy Principles*, all of which we encourage the Subcommittee to take into account as it considers incident reporting legislation and works on further refinements to the Act. We also led a recent multi-association letter to Congress stressing several key areas aligned with our principles that should be included in any incident reporting legislation.[2]

After briefly **providing important context to help inform the current security incident reporting debate**, I will focus the bulk of my written testimony **on five recommendations that were included in our *Policy Principles*,** as well as the above-referenced multi-association letter, including: 1) **establishing feasible reporting timelines** of no less than 72 hours; 2) ensuring appropriate **confidentiality, nondisclosure, and liability protections**; 3) **limiting reporting to the impacted organization**, rather than third-party vendors or providers; 4) **harmonizing federal cybersecurity incident reporting requirements**; and 5) **limiting reporting to verified intrusions** and incidents. My testimony concludes by **stressing the importance of seizing the opportunity to develop a workable security incident notification regime while preserving CISA's collaborative role** with private sector partners.

[2] Letter available here: https://www.itic.org/documents/cybersecurity/MultiassnLetter-SecurityIncidentReporting-08.27.2021FINALFINAL.pdf

I. Security Incident Reporting in Context

Devising a successful cybersecurity incident reporting regime requires an understanding of adjacent and overlapping cybersecurity information sharing and data breach notification measures, as well as the evolving global policy debates regarding this issue.

a. Clarifying and Understanding Terms Can Help Efficiently Harmonize Requirements

In thinking about security incident reporting, it is essential that policymakers and other stakeholders recognize that it is distinct from other concepts with which it is often confused: primarily, data breach notification and cybersecurity threat information sharing. Security incident notification such as that contemplated by the Act requires organizations to report on the details of a cybersecurity incident that has already occurred to help increase visibility into such events; data breach notification requirements are also triggered post-incident but relate specifically to reporting details regarding the unauthorized access to or disclosure of personally identifiable information or other sensitive data for privacy purposes. Importantly, policymakers should consider that in some instances a single incident could trigger both types of notification and reporting requirements and should consider how to reduce potential inefficiencies in reporting. Both of the preceding two concepts are distinct from cyber threat information sharing, which refers to the proactive sharing of threat information to help all entities better understand cybersecurity threats and take steps to prevent future cyberattacks. Given the Subcommittee's intent to leverage the *Cybersecurity Information Sharing Act of 2015 (CISA 2015)* in the security incident reporting context, including to extend *CISA 2015's* liability protections, it is critical to understand both the differences and similarities between the two concepts. We further elaborate on all three of these concepts in our *Policy Principles* (see Appendix A).

b. The Global Policy Debate Can Help Inform US Policy

ITI is an active participant in policy conversations on cybersecurity incident reporting globally. Indeed, it is not only the United States that is considering implementing a mandatory incident reporting regime. Europe, in the proposal for a revised *Network and Information Systems Directive (NIS 2 Directive),* as well as Australia, in their *Security Legislation Amendment (Critical Infrastructure) Bill of 2020*, which revises the *Security of Critical Infrastructure Bill of 2018,* are contemplating mandatory incident reporting as a way to increase government visibility into cybersecurity events.[3] We have similarly encouraged both the European Commission and the Australian Government to adopt the

[3] Security Legislation Amendment (Critical Infrastructure) Bill of 2020, first reading text, available here: https://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/r6657_first-reps/toc_pdf/20182b01.pdf;fileType=application%2Fpdf; proposal for NIS 2 Directive text, available here: https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union.

principles discussed in my testimony and referenced in ITI's *Policy Principles.*[4] These global efforts are relevant and important to consider as Congress seeks to develop legislation that establishes a mandatory incident reporting regime, as the Subcommittee acknowledges in the Act by requiring the CISA Director to align the reporting requirements CISA develops with international standards.

II. Recommendations for a Successful Security Incident Notification Approach

ITI's *Policy Principles* set forth ten recommendations that policymakers should incorporate to develop and implement a successful cybersecurity incident notification regime. While all of these recommendations are important, my testimony focuses on five key recommendations below. Please refer to the *Policy Principles* at annex for the full set of recommendations.

a. Establish Feasible Reporting Timelines

In our *Policy Principles*, we recommend that any legislation allow for reasonable reporting timelines commensurate with incident severity levels, but of no less than 72 hours. Ensuring that timelines are feasible is important for a number of reasons, including:

Allowing companies sufficient time to determine what has occurred. Requiring an entity to report an incident on a shorter timeline may be insufficient for companies to determine the nature of the issue – is it a cyberattack or is it merely a network outage? In the early hours following the discovery that something anomalous has occurred, our companies are focused on figuring out *what* has happened and developing a response plan. Indeed, the primary initial focus for companies should be on identifying and responding to malicious activities, rectifying the problem, and ensuring (or restoring) business continuity.

Upholding cybersecurity while a company investigates the issues. A shorter timeline for reporting may also serve to undermine cybersecurity, in that such a requirement can expose information about an incident before a patch is applied or operations are restored, making operators and their customers vulnerable to additional attacks by hackers.

Ensuring resources are leveraged appropriately and ensuring the incident is properly contextualized. Requiring reporting on a shorter timeline may also divert limited government resources away from addressing incidents that are actually having a significant impact. If entities are required to report incidents before they have the opportunity to verify what has occurred, an agency such as CISA runs the risk of being inundated with reports that do not offer meaningful information or otherwise lack the appropriate context. It is incredibly difficult to narrow the scope on the back end when an agency is sifting through reports trying to retroactively determine what is important. Instead, the

[4] ITI Comments on NIS 2 Directive, available here: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12475-Cybersecurity-review-of-EU-rules-on-the-security-of-network-and-information-systems/F2004660_en; ITI Comments on Security Legislation Amendment Bill of 2020, available here: https://www.aph.gov.au/DocumentStore.ashx?id=04c36c84-3067-4ffb-bec2-53c780079a02&subId=701444.

focus should be on only requiring incident reporting of severe and significant attacks that cause actual disruption or loss and that include specific parameters.

Aligning with global best practices. A 72-hour timeline also aligns with global best practices, which we believe is of great importance to facilitating interoperability of approaches. For example, the German *IT Security Act* and various state-level notification requirements in the United States allow for a reporting window of 72 hours.[5] Article 33 of the EU's *General Data Protection Regulation (GDPR)* also states that in the case of a personal data breach, impacted companies shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority.

We appreciate that as currently drafted, Subsection (d)(5) of the Act makes clear that the CISA Director may not require reporting any earlier than 72 hours after an entity has *confirmed* that an incident has occurred. We also stress that requiring a formal report on a verified, significant incident should not preclude an impacted organization from voluntarily providing less-fulsome notifications to CISA on a more flexible timeline. Indeed, should an entity want to notify CISA of an event before a formal report is finalized and submitted, it should have the ability to do so. Section (f) of the Act seems to contemplate such a layered approach, which would allow for an initial voluntary, preliminary notification to CISA, with more substantial reporting coming once the impacted organization has confirmed that an incident reached the severity metrics established in the IFR called for by the Act.

b. Maintain Appropriate Confidentiality, Nondisclosure, and Liability Protections

In ITI's *Policy Principles* we also stress the importance of ensuring the confidentiality of information provided in incident reports. It is imperative to have strong and transparent rules about the confidentiality of incident information that is shared with or by federal agencies in order to cultivate trust in the process and between the private and public sectors. Such rules should govern not only the dissemination of incident information with relevant interagency partners but should specifically preclude direct or indirect regulatory use of such information. Such rules should additionally govern how unclassified information on a specific incident is further shared with the US Government, other governments, and with nongovernmental entities. These rules must be crafted to guarantee compliance with existing legal regimes, including contractual and privacy obligations.

This is an area that we believe could be strengthened in the Act. Indeed, it is our view that the language surrounding how the information provided in an incident report can be used based on the Act's Subsection (e)(1) does not provide a sufficient level of confidentiality for

[5] German IT Security Act 2.0 available here: https://www.bundesrat.de/SharedDocs/beratungsvorgaenge/2021/0301-0400/0324-21.html; Regarding state level timelines, see, e.g., New York Department of Financial Services reporting requirements: https://www.crowell.com/NewsEvents/AlertsNewsletters/all/Newly-Proposed-Cyber-Reporting-Rules-for-Banking-Organizations

industry partners. The language lays out broad circumstances where information can be shared (*i.e.*, for a "cybersecurity purpose"), but it does not provide details as to how that information will be protected from disclosure. We believe that the Act should define clear confidentiality and privacy requirements regarding the use of such information and that it should require that any information that is further disseminated is scrubbed of all identifying information of the entity that provided it.

We also make the point in our *Policy Principles* that it is important that policymakers ensure that there are appropriate liability protections maintained in incident reporting legislation, so that information provided in a report cannot later be used against an entity. Of course, if there are instances in which entities have engaged in unlawful misconduct, such liability protections would not apply. We also believe that security incident reporting legislation should make clear that cybersecurity incident reports shared with the US Government should be exempt from FOIA requests. Given this recommendation, we welcome the Act's provisions in Section (f) which offer protection to entities that report or provide information under Section 106 of *CISA 2015*. At the same time – and this is an issue which extends beyond the specific legislation that is being considered at present – we believe that the language in *CISA 2015*, which is primarily limited to "cyber threat indicators," may well need to be updated to include the categories of incident reporting information that are ultimately required to be included in the reports submitted to CISA under the Act. Adding such definitional clarity to *CISA 2015* itself will help to ensure that entities receive liability protection for all relevant information that is shared, whether through voluntary cyber threat indicator sharing, or mandatory or voluntary incident reports provided to CISA under the Act.

c. Limit Reporting to the Impacted Entity

Another question that arises not only in the domestic conversation on incident reporting but in the global conversation as well is who is responsible for reporting an incident to the competent authority (CISA, in the case of the Act). We believe that the reporting obligation should fall only on the impacted entity, and that vendors or third-party service providers should not be required to report cybersecurity incidents to the US Government that have occurred on their customers' networks.

An incident reporting requirement with a broader scope would pose numerous challenges to many organizations' normal business operations, including potentially forcing vendors or third parties to disclose business confidential information of impacted customers or breach their contractual obligations. Such a requirement, if scoped broadly to incorporate third parties and vendors, may also result in duplicative incident reports which, as mentioned previously, could inundate CISA with multiple duplicative reports that they then must sift through, diverting limited resources away from meaningfully addressing significant cybersecurity incidents.

d. Streamline Incident Reporting Requirements

There are currently several different measures that govern federal cybersecurity incident reporting, making for a complex and often confusing landscape. Numerous federal agencies currently have disparate incident reporting requirements, many of which are just starting to be implemented. For example, the banking sector is subject to multiple specific notification requirements (see, e.g., *12 CFR part 30, appendix B, supp. A (OCC); 12 CFR part 208, appendix D-2, supp. A, 12 CFR 211.5(l), 12 CFR part 225, appendix F, supp. A (Board); 12 CFR part 364, appendix B, supp. A (FDIC) (italics omitted); NPRM on Computer Security Incident Reporting Requirements for Banking Organizations and their Bank Service Providers*) as is the defense industrial base (see *32 CFR § 236.4 - Mandatory cyber incident reporting procedures)*. There are also reporting requirements captured in FISMA (see 44 U.S.C. §§ 3553-54 & associated Binding Operational Directive 16-03); FedRAMP Incident Communications Procedures; NERC *Incident Reporting and Response Planning* as required by FERC; and the US-CERT Federal Incident Notification Guidelines. Additionally, Section 2 of the President's *Executive Order on Improving the Nation's Cybersecurity* includes a number of provisions aimed at improving incident reporting on the part of federal contractors. There may also be interactions with existing privacy reporting requirements or with law enforcement processes. And additionally, as alluded to above, various state laws impose data breach reporting requirements, often stemming from the same incidents.

To alleviate the confusion that is brought about by this complex incident reporting landscape, we urge Congress in our *Policy Principles* to harmonize existing regulatory reporting requirements to ensure that companies are more efficiently able to report incidents and are not subject to contradictory, duplicative, or otherwise confusing reporting requirements that may serve to hamper the notification process. We also recommend that reported information be aggregated, anonymized, analyzed, and shared in a manner that facilitates the mitigation and/or prevention of future cyber incidents.

All that being said, we appreciate that the Act recognizes in Subsections (d)(7)(A) and (B) that covered entities may be subject to existing regulatory requirements, and that it directs the CISA Director to consider those existing regulatory requirements in establishing reporting requirements for covered entities, including working with other regulatory authorities to see whether and how streamlining is feasible. While we appreciate the inclusion of this provision, the Act currently does little to actually lessen the regulatory burden. We recommend adding language that clarifies that CISA should leverage existing channels to collect incident information whenever possible, including having existing interfaces such as the FBI, SEC, and financial sector regulators provide updates based on engagement with the private sector. This could be accomplished by directing the Office of Management and Budget to issue guidance to federal regulators and law enforcement requiring agencies to share information related to covered incidents against covered agencies with the Cyber Incident Review Office.

e. Establish Appropriate Reporting Thresholds and Limit Reporting to Verified Incidents

We appreciate that the Act attempts to establish minimum thresholds for reporting a "covered incident" based on a risk-based, analytical model. We consistently encourage policymakers to take a risk-based approach to cybersecurity, and incident reporting is no exception. It is important that the threshold for requiring an incident report is sufficiently narrow and clearly delineated. Reporting requirements should include specific parameters and be mapped to objective criteria, and incident severity levels should be related to identifiable harms, such as to public health and safety, or operational disruption.[6] However, the considerations outlined in the Act's Subsection (4)(A) introduce ambiguity that is not resolved in the minimum threshold language outlined in Subsection (4)(B). Relatedly, providing additional rigor around what constitutes a "significant cyber incident" would be helpful.

In our *Policy Principles,* we recommend that policymakers explore the idea of an incident categorization matrix, which can represent the severity of an incident more accurately, therefore allowing for prioritization of incidents. We believe that a similar concept would be useful to introduce here and encourage the Subcommittee to include language that directs CISA, in conjunction with interagency partners, to develop such an incident categorization matrix. A categorization matrix can be used to help determine the severity of, and potential for, actual harm posed by an incident more accurately, helping to prioritize incidents and ultimately enabling more precise reporting. Focused reporting that is limited to severe incidents that may result in actual harm reduces the burden on information security teams and frees up resources for the essential tasks of examining and remediating incidents and securing an organization's systems.

Similar approaches have been proposed by CISA and have already been adopted by the United Kingdom (UK) and Australia. The UK's National Cyber Security Center developed a Cyber Attack categorization system, with incidents broken down into six categories, ranging from a category 1 national cyber emergency to a category 6 localized incident. Along with breaking out incidents into categories, the UK's matrix includes a definition of the type of incident, information about who responds to that incident, and what activities responders should undertake.[7] This approach helps lend additional clarity to determining the severity of an incident and allows for resources to be deployed more efficiently. Australia has developed a similar Cyber Incident Categorization Matrix, which lays out similar categories ranging from 1-6 and provides illustrative examples of the types of incidents and impacted entities that fall in a given category. This matrixed approach allows the Australian

---

[6] Currently, the US approach to categorizing cyber incidents in the National Cyber Incident Response Plan defines a "Significant Cyber Incident" as a cyber incident that is (or group of related cyber incidents that together are) likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.

[7] Overview of NCSC cyber categorization matrix available here: https://www.ncsc.gov.uk/news/new-cyber-attack-categorisation-system-improve-uk-response-incidents.

Cybersecurity Centre to triage incident reports and respond appropriately based on level of impact.[8]

We applaud the Committee's focus on incidents that produce actual harms as established by the minimum thresholds for a "covered cybersecurity incident" as set forth in Subsection (4)(b). This emphasis on incidents that cause disruption of business operations, compromises of the integrity or confidentially of data, and loss of services ensures CISA's limited resources can be effectively and efficiently leveraged. We were pleased to see that the Act focuses on such confirmed incidents, as we have observed a somewhat troubling trend in proposed incident reporting policies globally which require entities to report "potential" incidents or "near misses." In our view, requiring the reporting of "potential" incidents does little to improve cybersecurity and could inadvertently create an information overload, preventing the competent authority from prioritizing actual, confirmed incidents, and undertaking appropriate action to respond, particularly when it is not clear what would constitute a "potential" incident. As we noted in the multi-association letter and in our *Policy Principles*, reporting verified or confirmed incidents that have been well-defined and scoped will help to avoid a culture of overreporting that will strain limited incident response capacity and capabilities inside and outside the government. It will also help ensure that information received is useful and actionable.

III. Prioritizing Partnership and Collaboration Puts CISA in the Best Position for Success in Cyber Incident Reporting

ITI has long advocated that public-private partnerships are essential to improving cybersecurity, and CISA and its predecessor entities at the Department of Homeland Security have been established as key partners to industry on issues such as cybersecurity threat information sharing and supply chain risk management. These partnerships are essential to 1) identify potential threats; 2) understand how and to what extent risks can be managed; and 3) determine what actions should be taken to address risks without yielding unintended consequences. The Act we are discussing today acknowledges that government and industry often have access to unique information sets; this is certainly the case in the context of a security incident, which is why sharing or reporting certain categories of information can help all relevant stakeholders see the complete picture, increasing situational awareness and driving more effective operational collaboration in response to significant incidents.

The private sector ICT community has not only been foundational in developing the infrastructure of cyberspace but, for well over a decade, in providing leadership, innovation, and stewardship in all aspects of cybersecurity, including helping to develop and participating in numerous public-private partnership structures and efforts. For example, global ICT companies have long participated in sector coordinating councils (SCC), self-organized, self-governed councils that allow owners and operators of critical

[8] Matrix available at https://www.transparency.gov.au/annual-reports/australian-signals-directorate/reporting-year/2019-20-6.

infrastructure to engage on a range of cybersecurity strategies, policies, and activities with CISA and other US government counterparts, and also participate in the ICT SCRM Task Force launched in 2018. I am pleased to serve as the Vice Chair of the ITSCC and to work closely with my counterparts in the Communications SCC, as well as CISA and other U.S. government partners as co-chair of the ICT SCRM Task Force.

We believe that if an incident reporting regime is crafted carefully, it can be a helpful tool to improve federal agencies' situational awareness into cybersecurity incidents as well as to drive improvements in operational collaboration between CISA and industry. In order to realize such an effort, CISA's role as a trusted and collaborative partner to industry must be preserved, if not strengthened, as it must be able to continue to engage with relevant stakeholders, including critical infrastructure owners and operators, on not just the cybersecurity incident notification and reporting requirements contemplated here but on the array of other important and ongoing cybersecurity and supply chain risk management partnership activities referenced above.

This is an important moment in the history of CISA, still a relatively new agency that has had to adapt itself to meet what seems like a new set of threats and challenges every year. The legislation under consideration by this Subcommittee holds the promise of not only developing an effective and efficient cybersecurity incident reporting regime, but in doing so in a way that preserves the partnership and collaborative model that this Subcommittee set out when it created CISA three years ago. We urge the Subcommittee to ultimately adopt legislation that achieves both of these goals.

Conclusion

Members of the Subcommittee, ITI and our member companies once again commend you for your leadership on this issue. We appreciate your approach to engaging with stakeholders to ensure the partnership model that CISA was founded on will be protected and continue to evolve as it tackles these new threats. We encourage you to keep both the partnership model and goal of improving operational collaboration in mind as you consider how to best refine the Act in order to lend additional clarity to questions around issues including minimum thresholds for incident reporting, confidentiality and liability protections, and conflicting or duplicative reporting requirements.

ITI stands ready to provide the Subcommittee with any additional input and assistance as it seeks to develop an approach to cybersecurity incident reporting for critical infrastructure owners and operators. And we reiterate our request that the Subcommittee consider our full set of *Policy Principles,* which, when taken together, will help policymakers to structure a clear, straightforward incident reporting regime that provides actionable, appropriately contextualized information.

I would like to again thank the Chair, Ranking Member, and Members of the Subcommittee for inviting me to testify today and for your interest in and examination of this important issue. I look forward to your questions.

Thank you.

ITI Promoting Innovation Worldwide

Appendix A:

ITI Policy Principles for Security Incident Reporting in the U.S.

July 2021

The SolarWinds compromise has demonstrated how the cyber threat landscape is constantly evolving, resulting in the emergence of new threats. In search of a suitable policy response, policymakers have increasingly turned to incident reporting policy regimes as a potentially appropriate tool. The proposals introduced to date often conflate multiple issues and misunderstand the goals and the applicability of security incident reporting.

ITI recognizes the importance of cybersecurity incident reporting to inform actions to respond to incidents and to contain or prevent further impacts. ITI views the concepts related to security incident reporting as distinct from those of cyber threat information sharing or a data breach notification (see box for details). If a report provides sufficient technical details about the suffered incident, federal agencies can understand the nature of the attack and take steps to mitigate the associated risk. Likewise, actionable reporting may help government officials to prioritize incident response assistance to affected organizations, particularly while dealing with an active campaign targeting multiple organizations. This assumes that affected organizations required support and that the principles articulated below have been fully adopted.

As such, if carefully crafted, incident reporting has the potential to be a helpful policy lever. It is through this lens that we offer our recommendations on several key areas that policymakers should consider in developing an effective, efficient security incident reporting regime.

Security incident reporting is distinct from other concepts with which it is often confused: data breach notification and cyberthreat information sharing. While some incidents may blur the line between these concepts, it is important to understand the difference between these terms and what each process is meant to achieve.

Security Incident Reporting *focuses on the past because it reports on the details of a cybersecurity incident that has already occurred. This could include the vector of compromise, the systems and information compromised or targeted by the attacker, and any attributes of the attacker's behavior. Reports may focus on the actual or the potential harm caused by an incident. Information conveyed in the reporting highly depends on the reporting timeline, reporting purpose (and use) and segment needs.*

Data Breach Notification *relates specifically to the unauthorized access to or disclosure of personally identifiable information or other sensitive privacy data. In the United States, there are more than 50 state and local laws focused on data breach notification.*

Cyberthreat Information Sharing *focuses on the future and refers to the proactive sharing of threat information to help all entities understand threats and take steps to prevent successful cyberattacks. Threat information sharing should be voluntary and may include indicators such as anomalous network activity or methods of circumventing security controls.*

Develop and Adopt an Incident Categorization Matrix

Global Headquarters
700 K Street NW, Suite 600
Washington, D.C. 20001, USA
+1 202-737-8888

Europe Office
Rue de la Loi 227
Brussels - 1040, Belgium
+32 (0)2-321-10-90

info@itic.org
www.itic.org
@iti_techtweets

Policymakers should ensure that the threshold for reporting requirements is mapped to specific objective criteria and specific incident severity levels related to identifiable harms, such as to public health and safety, or operational disruption.[1] Reporting requirements should only focus on severe and significant attacks that cause actual disruption or loss and should include specific parameters. An incident categorization matrix[2] can represent the severity of an incident more accurately which helps with the prioritization of incidents and ultimately supports more precise reporting. Focused reporting that is limited to severe incidents reduces the burden on information security teams and frees resources for the essential tasks of examining and remediating incidents and securing the organization's systems. Moreover, it reduces the likelihood of an informational overload for applicable authorities that would undermine their ability to prioritize responses and divert limited agency resources from critical risk mitigation activities. These considerations are also key in the context of defining the scope and object of reporting (e.g., avoiding the confusion of 'incident' with other concepts or expanding to 'potential' incident reporting). We recommend policy makers advance the joint understanding of the matrix and severity concept, by facilitating a consensus-driven processes.

Establish Feasible Reporting Timelines Commensurate with Incident Severity Level

Any incident reporting legislation should ensure that timelines are aligned with global best practices. The required timelines should be commensurate with incident severity levels but allow for at least a 72-hour reporting window after an entity has verified the incident. Anything shorter is unnecessarily brief and injects additional complexity at a time when entities are more appropriately focused on the difficult task of understanding, responding to, and remediating a cyber incident. Shorter timelines also greatly increase the likelihood that the entity will report inaccurate or inadequately contextualized information that will not be helpful, potentially even undermining cybersecurity response and remediation efforts.

Limit Responsibility for Reporting Only to the Compromised Entity

Any legislation should ensure that the reporting obligation falls only on compromised entities. Vendors and third-party service providers should not be required to report cybersecurity incidents to the US Government that have occurred on their customers' networks. Such a requirement would pose numerous challenges to normal business operations, including potentially forcing vendors or third parties to disclose business confidential information of that customer or breach their contractual obligations.

Ensure Confidentiality and Appropriate Protections around Sensitive Information Shared with Federal Agencies, including Against Regulatory Use

It is imperative to have strong and transparent rules about the confidentiality of incident information that is shared with or by federal agencies. Such rules should govern not only the dissemination of incident information with relevant interagency partners but should specifically preclude direct or indirect regulatory use of such information. Such rules should additionally govern how unclassified information on a specific incident is further shared with the US Government, other governments, and with nongovernmental entities. These rules must be crafted to guarantee compliance with existing legal regimes, including contractual and privacy obligations. A designated centralized reporting agency

[1] Currently, the US approach to categorizing cyber incidents in the National Cyber Incident Response Plan defines a "Significant Cyber Incident" as a cyber incident that is (or group of related cyber incidents that together are likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.

[2] Similar approaches have been proposed by CISA and are already adopted by the UK and Australia.

should provide a secure method of communication. This could be as simple as publishing a PGP encryption key or using the Traffic Light Protocol (TLP). Trust is essential.

Establish Targeted Liability Protections and Appropriate Exemptions from the Freedom of Information Act (FOIA)

Entities providing incident reports should receive liability protections for providing such information to federal agencies, including engaging in activities related to monitoring or network awareness of their information systems, other than in instances where entities engage in willful misconduct. Additionally, cybersecurity incident reports shared with the US Government should be exempt from FOIA requests.

Harmonize Federal Cybersecurity Incident Reporting Requirements

There are currently several different measures that govern federal cybersecurity incident reporting, making for a complex and oftentimes confusing landscape.[3] To alleviate such confusion, Congress should consider harmonizing existing regulatory reporting requirements to ensure the efficient sharing of covered cybersecurity incidents.

Designate a Single Point of Contact for Companies to Report Security Incidents to within the Government

Incident response and recovery resources are in short supply. To effectuate the efficient use of limited resources, the federal government should designate, and adequately fund, a single point of contact for all companies that need to report an incident. If existing reporting requirements have not been harmonized and sector-specific reporting requirements remain in place, impacted organizations should not be required to report an incident twice. All future legislative proposals should designate CISA as the single point of contact where no sector-specific regulator exists, and appropriate resources should be allocated for that purpose.

Define an Appropriate and Flexible Reporting Template

All incident reports should follow a standardized template to ensure consistent reporting across agencies and industries. Consensus-driven processes are needed to refine the elements of such a template to ensure consistency with existing frameworks, like MITRE ATT&CK or VERIS, and international industry best practices, as well as to ensure that the template fits the needs and existing practices of a particular sector. Reporting entities can use such a template to report the most relevant information where available. By way of example, the template may include appropriate and reasonably obtained information on 1) the attack vector or vectors that led to the compromise; 2) the indicators of compromise; information on the affected systems, devices, or networks; 3) information relevant to the identification of the threat actor or actors involved; 4) a point of contact from the affected entity; and 5) impact, earliest known time, and duration of compromise.[4] Entities should have the option to report additional types of information on cybersecurity incidents to help to identify emerging trends or

---

[3] See, for example, banking sector notification requirements: *12 CFR part 30, appendix B, supp. A (OCC); 12 CFR part 208, appendix D-2, supp. A, 12 CFR 211.5(l), 12 CFR part 225, appendix F, supp. A (Board); 12 CFR part 364, appendix B, supp. A (FDIC) (italics omitted); NPRM on Computer Security Incident Reporting Requirements for Banking Organizations and their Bank Service Providers;* defense industrial base mandatory reporting requirements: *32 CFR § 236.4 - Mandatory cyber incident reporting procedures;* FISMA reporting requirements: 44 U.S.C. §§ 3553-54 & associated Binding Operational Directive 16-03; FedRAMP Incident Communications Procedures; NERC *Incident Reporting and Response Planning* as required by FERC; and US-CERT Federal Incident Notification Guidelines.

[4] This initial list is based on the following CISA documents: https://www.cisa.gov/sites/default/files/publications/Law%20Enforcement%20Cyber%20Incident%20Reporting.pdf https://www.cisa.gov/sites/default/files/publications/Non-Federal%20Entity%20Sharing%20Guidance%20under%20the%20Cybersecurity%20Information%20Sharing%20Act%20of%202015_1.pdf; other resources are available: https://us-cert.cisa.gov/sites/default/files/publications/Federal_Incident_Notification_Guidelines.pdf.

otherwise preempt attacks. Entities should also not be penalized for or precluded from reporting an incident if all information, including the information proposed in this list, is not available.

Align Reporting Processes and Mechanisms to Ensure Consistency with Industry Best Practices and Allow for Bi-Directional Information Sharing

The protocols and mechanisms of reporting an incident should be consistent with existing frameworks, recognized sectoral, international, and industry best practices. To ensure incident information is shared quickly and continuously, sections 2.f and 2.g of Executive Order 14028 direct improvements to the inter-agency sharing of incident information. In addition to these provisions, federal agencies also need to streamline legal agreements involving industry partners to allow for bi-directional sharing of incident information.

Build Agency Capability to Act on Security Incident Reports

Security incident reporting will be of limited utility if the designated recipient agency does not have the capacity to ingest and act on the information it receives. A manual-intensive approach will quickly max out resources and elevate the risk that important alerts are inadvertently missed. Before a security incident reporting scheme is established, the designated recipient agency should have the capability to automate data collection so that internal data can be cross-referenced with externally available data. This will inform and improve the orchestration of incident response actions.