Cybersecurity (H) Working Group

Virtual Meeting

November 16, 2023

Consider the Adoption of the Summer National Meeting Minutes

Draft: 4/6/23

Cybersecurity (H) Working Group
Virtual Meeting (*in lieu of meeting at the 2023 Spring National Meeting*)
March 7, 2023

The Cybersecurity (H) Working Group of the Innovation, Cybersecurity, and Technology (H) Committee met March 7, 2023. The following Working Group members participated: Cynthia Amann, Co-Chair (MO); C.J. Metcalf, Co-Vice Chair (IL); Michael Peterson, Co-Vice Chair (VA); Julia Jette (AK); Damon Diederich (CA); Wanchin Chou (CT); Tim Li (DE); Shane Mead (KS); Matt Kilgallen (GA); Daniel Mathis (IA); Alexander Borkowski (MD); T.J. Patton (MN); Jake Martin (MI); Troy Smith (MT); Colton Schulz and Chris Aufenthie (ND); Martin Swanson (NE); David Bettencourt (NH); Justin Herrings (NY); Matt Walsh (OH); John Haworth (WA); and Rebecca Rebholz (WI).

1. Adopted its 2022 Fall National Meeting Minutes

Haworth made a motion, seconded by Schulz, to adopt the Working Group's Nov. 15, 2022, minutes (see NAIC Proceedings – Fall 2022, Innovation, Cybersecurity, and Technology, Attachment Three). The motion passed unanimously.

2. Discussed its Work Plan for 2023

Amann summarized the Working Group's work plan for 2023 (Attachment Two-A) The work plan contains four components, called workstreams, building from the results of the Working Group's survey to state insurance regulators in 2022.

The first item on the work plan is to develop a cybersecurity response plan. The subject matter expert (SME) group leads for this workstream are Amann and Peterson. The outline for the response plan includes 12 topics to date:

- Introduction
- Communication with other states/federal regulators
- Initial notification by domestic
- Meetings (initial and follow-up meetings if necessary)
- Communication with the firm handling the incident
- Organizational security
- Risk assessment
- Audits
- Communications with consumers
- Summary of regulator tools
- Coordination of communication
- Information-gathering template

A drafting group is being formed, and drafting will begin following the Spring National Meeting.

The second item on the work plan is for the Working Group to send a referral to the Information Technology (IT) Examination (E) Working Group asking it to consider updating its cybersecurity guidance (Attachment Two-B).

© 2023 National Association of Insurance Commissioners

The third item on the work plan is for the Working Group to continue to support NAIC training initiatives. This workstream will identify cybersecurity subject matters. The Working Group will work with NAIC staff, state insurance regulators, and the insurance industry to identify warranted training. Any work considered by this workstream requires coordination with the Innovation, Cybersecurity, and Technology (H) Committee to avoid duplications of effort.

The fourth item on the work plan is for the Working Group to continue to monitor cybersecurity trends among regulated entities and among federal and international bodies. State insurance regulators will receive relevant updates regarding cybersecurity trends, work being completed by related working groups, state efforts to adopt the *Insurance Data Security Model Law* (#668), and relevant work happening at the federal and international levels.

Amann concluded by asking states to consider volunteering and contacting NAIC staff with their specific interest in supporting components of the work plan. Romero noted that workstream one, the cybersecurity response plan, is the workstream most likely to need assistance. Romero acknowledged past willingness to aid from Connecticut and North Dakota.

Haworth asked if the Working Group would meet in regulator-to-regulator session to discuss cybersecurity events. Amann said there may be a case for regulator-only sessions for some of the issues the Working Group will be addressing. Romero indicated that if there is a specific subject matter related to an examination or another confidential matter, a regulator-only meeting would be a possibility.

3. Heard an Overview of the Treasury Department's Report Titled *The Financial Services Sector's Adoption of Cloud Services*

Ethan Sonnichsen (NAIC) provided an overview of the U.S. Department of Treasury's (Treasury Department's) *The Report on the Financial Services Sector's Adoption of Cloud Services*, which was released on Feb. 8. The report discusses the benefits and challenges of the financial services sector's increasing adoption of cloud services technology. It also makes several recommendations for financial service providers and the regulatory community.

The report summarizes some of the benefits, including scalability, cost savings, and the security of the information technology infrastructure. In the financial services sector, there is a concentration among a small number of cloud service providers. Risks may involve a significant system failure or data breach at a large cloud service provider, which may have substantial implications for the financial services sector and the customers they serve. Many financial services institutions additionally expressed concerns regarding a cloud service provider's (CSP's) cybersecurity vulnerabilities. Currently, there is a lack of data in the financial regulatory community regarding the number of providers and the types of services provided at CSPs.

The report addressed concerns from institutions regarding the lack of transparency of reporting, as several of the institutions surveyed noted they do not receive information regarding incidents, outages, or other problems at the CSP that would affect the institution's system or its customer's access to information.

The report highlights a talent gap at financial services firms, including training expertise and the ability to determine which services to transition to a cloud infrastructure. The talent gap is the most pressing issue for smaller institutions.

The report also notes there is exposure to potential operational incidents at CSPs. Many financial services institutions additionally expressed concerns regarding CSPs' cybersecurity vulnerabilities or a service failure. Financial service regulators need more data regarding a financial institution's exposures.

Additionally, the report addresses the global regulatory requirements and how those may create challenges for firms wishing to migrate to a cloud service. There are regulatory differences around the world, making it difficult for a large global financial institution wanting to transition to the cloud. Some countries have restrictive data policies requiring data to be housed locally, whereas the U.S. is less restrictive regarding data flows.

Likewise, the report addresses concerns regarding market concentration. First, the market is concentrated among a small number of CSPs; third-parties may also use the same CSP. This concentration means an incident has a better chance of spreading throughout the financial system. Market concentration exists across banking, securities, and insurance markets. There is also a need to close significant data gaps regarding a financial institution's use of a CSP to better understand its risk exposure.

The report asks financial institutions to think about building a communication plan with its CSP, establishing a risk management framework to prioritize which systems will move to the cloud, whether there are backups and controls to execute them, and to introduce performance metrics showing the financial institution is receiving some economic value by transitioning to the cloud.

A cloud services steering group will be created in the next year or so to focus closer on domestic collaboration among financial regulators regarding cloud services. The steering group will consider writing best practices for cloud adoption and cloud contracts to provide some standardization. Interagency collaboration and coordination will be important. The steering group will also examine the data gap regarding CSP usage and determine what the financial regulators need to know regarding the reliance at a CSP.

The steering group will also look at protocols for incident response and engaging on international standards as the international standard setting groups, as well as fostering some industry discussions to obtain a direct account of what is happening in the financial services sector as cloud standards are adopted.

Amann asked the Working Group to consider the data state insurance regulators need, why they need it, and what the data will disclose regarding an insurer's use of cloud service providers. She asked the Working Group to also think about how this data is best obtained, whether the data is confidential data, unidentified data, group data, individual insurer data, how frequently the data needs to be collected, and if there are exemptions.

Peterson said that he believes the Treasury Department intends to remain active on this topic. He suggested that state insurance regulators could take the initiative to create a solution that works for both insurers and state insurance regulators. Peterson proposed that state insurance regulators use the systems summary grid, a tool in the *Financial Condition Examiners Handbook*, to help gather information on insurers' industry-wide use of cloud service providers. He suggested that a regulator-only filing submission could be beneficial as a new annual filing and would help regulators from a macroprudential perspective of an insurers' cloud service usage. There would be logistics to work through, including whether template standardization is necessary. Peterson asked the Working Group to consider whether this is a viable path forward to help state insurance regulators gather cloud service provider information.

Romero restated the proposal regarding whether regulators could use the systems summary grid to streamline the transmission of information on an insurer's use of cloud service providers, including whether data is needed and how frequently data needs to be submitted. Amann emphasized the need for insurers' input on this proposal. Romero indicated that given the time left for the meeting, the Working Group could solicit industry input on this proposal via e-mail following the meeting. Upon receiving the insurer's input, the Working Group could reconvene to continue the discussion.

© 2023 National Association of Insurance Commissioners

4. Discussed a Referral to the IT Examination (E) Working Group.

Amann said that because of the discussion last year with the Cybersecurity and Infrastructure Security Agency (CISA), the Working Group will be asking the IT Examination (E) Working Group to consider updating its cybersecurity-related guidance based on the CISA cybersecurity performance goals. Romero indicated that the Working Group has a charge to monitor and not to update cybersecurity guidance. Therefore, the referral sends the matter to the Working Group, having authority over cybersecurity guidance.

The Working Group's referral acknowledges there may be resources apart from the CISA cybersecurity performance goals. Updated guidance could help ensure the addressing of cybersecurity-related risks.

Brian de Vallance (Center for Internet Security—CIS) stated that cybersecurity is an important topic for state insurance regulators to consider and that the CIS supports updating the guidance as cyber defense has evolved. He noted that the CIS would be available to assist state insurance regulators as they continue to study this project.

5. Discussed the Outline for the Incident Response Plan

Amann stated that the Working Group's charge of creating an incident response plan builds on the Model #668 and would aid the states in requesting information from insurers that have experienced a cybersecurity event.

Amann indicated that insurers' input benefits this project, specifically in addressing the type of information that would be available. Romero indicated that in following up with states regarding the state insurance regulators' needs, the survey identified the demand for a tool assisting states in responding to cybersecurity events among regulated entities. Such a tool would help guide states in the communication and information-gathering responsibilities of the department of insurance (DOI). The tool would enhance a state's ability to act as a lead state in a cybersecurity event and minimize state inquiries to regulated entities.

States could tailor the tool to suit their individual needs. Romero suggested the Working Group form a drafting group to advance the tool's planning and suggested creating an information-gathering template and the value therein from an insurer's perspective.

Peter Kochenburger (University of Connecticut School of Law) said consumer representatives might also provide valuable input to ensure consumer notifications are included in the response plan. Schulz suggested that the workstream leverage insights from past NAIC cybersecurity tabletop exercises to assist with this project.

6. Discussed Other Matters

Skyler Gunther (NAIC) said that the NAIC would lead an effort to facilitate vendor presentations from Security Scorecard and Bitsight to provide information to state insurance regulators regarding cyber-risk analytic capabilities. Herring indicated that the New York Department of Financial Services (DFS) has been using Security Scorecard and may provide beneficial information in the Working Group's consideration of these tools. Romero indicated that after the vendor meetings, the state insurance regulators would reconvene to consider the usefulness of these tools.

© 2023 National Association of Insurance Commissioners

Discuss Comments Received and Receive an Update on the Cybersecurity Event Response Plan (CERP) Drafting Group and Discuss the CERP Draft

/2Y YŜyűă wŜŎŜƛØŜŘ ŦNJ2Y Y

! / [L

! I Lt

! t /L !

b ! a L /

Kirsten Wolfford
Counsel, ACLI
202-624-2059 t
kirstenwolfford@acli.com

November 3, 2023

Cynthia Amann and Gille Ann Rabbin, Co-Chairs, NAIC Cybersecurity (H) Working Group
Via email to Miguel Romero (maromero@naic.org) and Sara Robben (srobben@naic.org)

Re: Cybersecurity (H) Working Group Exposure Draft of the NAIC's Cybersecurity Event Response Plan (CERP)

Dear Cynthia Amann and Gille Ann Rabbin:

The American Council of Life Insurers (ACLI)[1] values the opportunity to respond to the Cybersecurity (H) Working Group's Exposure Draft of the NAIC's Cybersecurity Event Response Plan (CERP). The ACLI recognizes the threat cybersecurity events can pose to insurance companies and consumers. We support the work the NAIC is doing to combat this threat through coordinated cybersecurity oversight and guidance.

Cybersecurity Event Response Plan

We appreciate the Working Group's efforts to provide a uniform approach to cybersecurity event reporting and response with a documented Event Response Plan. A fully developed plan prior to implementation is key to this endeavor and the guidance included in the Event Response Plan should align with this goal. By clearly communicating this Event Response Plan to regulators and licensees, uniformity will be promoted.

We greatly appreciate the consideration and thoughtfulness that went into the current draft, but further information is needed to promote uniformity and consistency where possible across states. By creating more uniform processes, we avoid licensees responding to numerous regulators operating on different timelines using different procedures which can lead to consumer harm. We also recommend including a section in the Event Response Plan to assign responsibility and delineate a process for regular review and update.

[1] The American Council of Life Insurers (ACLI) is the leading trade association driving public policy and advocacy on behalf of the life insurance industry. 90 million American families rely on the life insurance industry for financial protection and retirement security. ACLI's member companies are dedicated to protecting consumers' financial wellbeing through life insurance, annuities, retirement plans, long-term care insurance, disability income insurance, reinsurance, and dental, vision and other supplemental benefits. ACLI's 280 member companies represent 94 percent of industry assets in the United States.

ACLI's specific feedback is included below under the headings included in the Draft:

Introduction
We appreciate the effort to emphasize the importance of clearly defined roles within DOIs. It is essential that the Response Plan be tightly focused on actions and considerations that must be made in the immediate days and weeks following a cyber event. Clearly understood roles will improve task execution, facilitate communication between stakeholders, and promote speed in securing vulnerabilities and mitigating any damage done.

Scope
The ACLI has no comment on this section.

Forming a Team and Communicating with Consumers
Overall, we support as uniform and consistent of an approach as possible. In addition to encouraging DOIs to implement clear guidance for consumer communications, a provision should be added to address inconsistent and sometimes duplicative notifications to consumers which can cause confusion for consumers and unfair reputational harm to licensees.

Communication with Law Enforcement and Other Regulators
The Event Response Plan should address these communications with enough specificity to provide clear guidance to DOIs. ACLI recommends that communications with other state and federal regulators should initially be confined to those communications required by law and/or needed to prevent the spread of a cybersecurity event. Any communications should be carefully secured so that the incident is kept confidential.

Understanding and Receiving Notifications
We appreciate the acknowledgement that during the information-gathering process, information may be given in parts and may change as the licensee's investigation proceeds. To address the varying state methods used to notify a regulator of a cybersecurity event, any guidance included in this section should prioritize the security of the information reported. In addition, guidance should direct regulators to internally share information on a "need to know" basis and provide best practices on data security and record retention.

Process for Responding to Cybersecurity Events
The process for responding to a cybersecurity event necessitates clear instructions on who should be leading communications, an understanding of the time development aspect of these incidents, and clear instructions on what is necessary to publish and what is not. In handling communications with a licensee, regulators should ensure they are communicating through the licensee's named lead contact person so that regulators receive secured, up-to-date, accurate information. To accommodate the time it takes to receive information related to a cybersecurity event, DOIs should refrain from publishing event information that does not add to meaningful consumer or industry protections (e.g., impacted licensee names).

How to Receive Notifications and Acquire Required Information

Any process for receiving notifications should contain adequate protections for the information being shared both during the sharing process and after. ACLI recommends the notification process:

- Include adequate protections of information submitted both during and after the notification process.
- Focus on containing initial notification to only the most pertinent information that is material to consumers and, thus, necessary to convey.
- Be clearly communicated by regulators via posted instructions on state webpages accessible to licensees, for how and where notifications should be submitted.

We suggest a lead state approach to simplify notification requirements and create further consistency in reporting across states.

Given that licensees rely on outside counsel to provide legal advice which is privileged and confidential, we do not suggest that DOIs make direct contact to licensee's outside counsel or to their third-party mitigation firm, if any, with a form requesting information. Instead, any DOI requests should be submitted through the licensee so that privilege can be maintained.

Appendix A: Sample Template

To protect confidential information shared with regulators in the case of a cybersecurity event, the Plan should reiterate that information shared on any form is protected and secured within DOIs. Additionally, although this is a sample template, this template could be a great opportunity for further uniformity across states. By creating a more uniform template, licensees can respond to cybersecurity events with much more efficiency, accuracy, and consistency across states.

Other Concerns

The draft does not appear to consider vendor cybersecurity events, which complicates the notification process. If the event occurs at a third party, the licensee needs to rely on the third party to provide information and respond to regulator questions. This might cause delays or less robust responses. ACLI recommends the inclusion of an additional provision to address these types of cybersecurity events and the additional timing considerations involved.

Conclusion

ACLI members recognize their affirmative obligation to maintain operations and protect consumer information amidst increasing cybersecurity threats. A united regulator and industry partnership is the best way to counter these threats. As such, we appreciate the collaborative approach the Working Group is taking on its ongoing cybersecurity oversight and regulation of the insurance industry. We encourage an ongoing dialogue between regulators and industry on cybersecurity issues to help both regulators and the industry better understand the other's underlying concerns, objectives, and challenges.

Thank you for your consideration of our comments. We welcome any questions.

Sincerely,



Kirsten Wolfford

Counsel, Cybersecurity Working Group Lead, ACLI

November 3, 2023

Cynthia Amman, Co-Chair
Gille Ann Rabbin, Co-Chair
Cybersecurity (H) Working Group
National Association of Insurance Commissioners
1100 Walnut Street, Suite 1500
Kansas City, MO 64106-2197

By Email to Miguel Romero at MARomero@NAIC.org

Re: AHIP Comments – Cybersecurity Event Response Plan (CERP) 10/3/23 Exposure

Dear Co-Chairs Amman and Rabbin:

On behalf of the members of AHIP, we appreciate the opportunity to provide comments on the October 3, 2023, Exposure Draft of the Cybersecurity Event Response Plan (CERP). AHIP is the national association whose members provide health care coverage, services, and solutions to hundreds of millions of Americans every day. We are committed to market-based solutions and public-private partnerships that make health care better and coverage more affordable and accessible for everyone by leveraging, among other things, technological solutions. Cybersecurity is an integral element of those solutions.

Our first concern pertains to the Scope paragraph on the first page. In the hectic events usually surrounding a Cybersecurity Event, it would be helpful to remind regulators to be aware not only of the reporting requirements in their state's insurance code, but also to other often overlapping laws such as the states' Attorneys General breach reporting laws and regulations, HIPAA, GLBA, the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), and the Federal Trade Commission's Health Breach Notification Rule.

We understand regulators' desire to have additional tools and guidance to assist them in the event a Cybersecurity Event is reported. However, AHIP members are concerned that in the regulators' desire to understand what happened, how it happened, how many consumers are impacted, and steps taken by the licensee to remedy any vulnerability of the licensee's systems leading to the Event, the quest for information may impede the critical functions the licensee

must perform to develop their own understanding of the incident and mitigate the incident and any impacts to consumers, including identification and notification of the impacted consumers. These concerns are heightened by the obligations noted in this letter's second paragraph, above.

However, we also believe these concerns are at least partially addressed in the NAIC Insurance Data Security Model Law (#668) itself in 6.B, requiring Licensees reporting a Cybersecurity Event to provide information in their notice to the Commissioner, "…as much…information as possible." This language acknowledges that the Licensee may make an initial report to the Commissioner before some, or even most, of the details are known.

We are pleased to see this reinforced in the CERP which cites this same language at the top of its page 2. Similarly, on page 1, the section Understanding and Receiving Notifications notes "…states should be mindful that partial information may be available, and information provided may changes as the licensee's investigation into the event proceeds." The CERP also notes in the first sentence in the Process for Responding to Cybersecurity Events section on page 3, that a DOI's information-gathering process should be able to proceed "without unduly burdening the licensee". In that same section the CERP also provides that in certain circumstances, "…the DOI may let the licensee's investigation run its course before stepping in to obtain the necessary information."

Lastly, we note with approval the mention of the importance of maintaining confidentiality during the DOI's response in the MO/VA/NAIC amended language added to page 4 of the draft CERP. It is critical to maintain the confidentiality of not only the information that may have been compromised, but also the details of how it occurred, and the steps taken by the company to avoid a repetition. This is essential for the protection of the licensee's information and that of consumers alike. AHIP would suggest language highlighting the importance of that confidentiality especially in situations in which the Commissioner shares information with a third-party consultant, since the statutory protections in Model 668 (or a state's enactment of it) which extend to material in the hands of the Commissioner might not be so clearly stated to extend to material held by a third-party. Without clear statutory language and authority, a third party's written agreement which contains promises to maintain confidentiality might not withstand a subpoena or other legal challenge.

Thank you for the opportunity to provide these comments, and we look forward to further discussing these matters with you.

Sincerely,

Bob Ridgeway
Bridgeway@ahip.org
501-333-2621



November 3, 2023

Chair Cynthia Amman
National Association of Insurance Commissioners
1100 Walnut Street, Suite 1500
Kansas City, MO 64106
Via email to Miguel Romero and Sara Robben

RE: Comments regarding NAIC Draft Cybersecurity Event Response Plan Exposure

Dear Chair Amman,

The American Property and Casualty Insurance Association (APCIA) appreciates the opportunity to provide comments in response to the exposure of the Cybersecurity Incident Response Plan (CERP).

APCIA is the primary national trade association for home, auto, and business insurers. APCIA promotes and protects the viability of private competition for the benefit of consumers and insurers, with a legacy dating back 150 years. APCIA members represent all sizes, structures, and regions—protecting families, communities, and businesses in the U.S. and across the globe.

We appreciate the opportunity to share APCIA's perspective of the draft Cybersecurity Event Response Plan (CERP) Exposure. In general, APCIA members are very supportive of the CERP, both in its intent and in its execution. APCIA has included some general feedback below on the Exposure, as well as a few specific proposed edits, outlined below. We hope that this feedback may be helpful in finalizing the CERP, as well as in informing the next steps of the Cybersecurity (H) Working Group.

General Feedback

Standardized Intake Form: APCIA members noted that it may be helpful for the NAIC to develop a standardized intake form, since many states differ significantly in the form and manner. Although our members appreciate that there are state statutory differences, to the extent possible a common type of form would be an improvement.

Confidentiality: Our members were supportive of the added confidentiality language that was provided in the updated CERP. It makes sense to reinforce the sensitivity of some of the information that insurers may be requested to report.

Communicating with Consumers: APCIA requests that it be clarified in the "Forming a Team and Communicating with Consumers" and "Understanding and Receiving Notifications" sections that a state insurance department should coordinate with and follow the lead of the affected licensee

prior to any consumer communication. Individual state data breach statutes most often require the data owner to notify affected individuals. Additionally, if the cyber event originated at a vendor, the notification obligations are more complex and certain contractual and legal obligations may need to be followed.

During an event and immediately thereafter, there is a great deal of activity going on to make sure systems are protected and all notification obligations are appropriately met, including to consumers. It would be helpful to have the affected licensee and all involved regulators speaks as "one voice" through consistent and uniform communication, thereby avoiding a potential unintended consequences of consumer confusion. Additionally, inconsistent, and sometimes duplicative, notifications to consumers may unfairly harm insurers' reputations, and the industry at large, without meaningfully helping consumers. Therefore, we respectfully request the CERP clearly explain the importance of coordinated communication and following the affected licensee's lead. The intake form could ask which state insurance departments are being notified, which would allow the notified departments to know with which of their peers to coordinate, saving time for both themselves and uninvolved departments.

APCIA members also think it is important that state insurance departments refrain from publishing incident information that does not add any actionable and meaningful consumer or industry protections (e.g., impacted licensee names).

Coordination Between Insurance Departments: It would be helpful if a domestic insurance department could coordinate with other state insurance departments to take the lead on investing multi-state cybersecurity events which also impact the domiciliary state. This would help to streamline the ongoing reporting requirements and minimize associated costs.

Security of Reported Information: The CERP indicates that reporting via email or pdf is acceptable. However, the nature of the information dictates that a secure portal is warranted at the very least. Given the sensitivity of the information, it is important that state insurance departments take action to ensure the privacy and security of the reported information. Broad knowledge of the specifics of an event can unnecessarily expose sensitive incident data and have devastating consequences for the licensee and insureds.

Specific Proposed Edit

P.4 "How to Receive Notifications and Acquire Required Information": Our members believe that an email or online form is insufficiently secure for reporting the information requested. A "secure" portal should be the minimum expectation, rather than the maximum. A breach of security that exposes reported information about cyber events would put licensees at even greater risk, and would therefore expose insureds to greater potential harm.

At a minimum, APCIA suggests the following additional language (at the bottom of page 4:

(1) "Before a cybersecurity event, DOIs should take reasonable steps to ensure they have the proper communication and security protocols and tools in place if the transmission of information

is necessary." and

(2) "Communication channels established for event notification should provide reasonable security of the data in transit and at rest, commensurate with the sensitivity of the reported information."

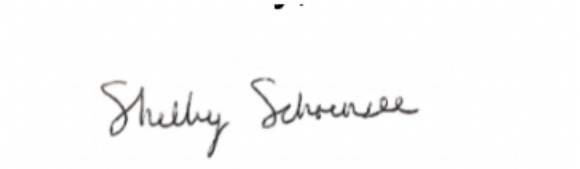
Conclusion

Following a widespread incident, licensees may be required to respond to multiple regulators and law enforcement units operating on different timelines and using different procedures. This creates a multi-pronged and substantial burden for the licensee, delays responses, and can lead to greater harms for the consumer. When speed is critical following a cyber event, licensees want to ensure they can focus their finite resources on customer communications, mitigation efforts, and fixing the underlying vulnerability, rather than navigating numerous and differing state-specific notification requirements. Updates to the regulatory process that allow insurers to notify efficiently and effectively, rather than navigating a confusing regulatory landscape, will ultimately allow licensees to ensure their finite time and resources are directed in the most effective ways in the wake of a breach.

APCIA suggests that the industry would benefit from something actionable that states might adopt and implement directly. For this reason, our members support simplified notification requirements, including supporting a lead state approach. APCIA hopes that these considerations may inform the NAIC Cybersecurity Working Group's continued work moving into next year.

APCIA thanks the Working Group for its consideration of our comments. We are happy to discuss any of the suggestions included herein further and appreciate this Working Group's efforts to create greater harmonization around cybersecurity event response.

Sincerely,



Shelby Schoensee
Director, Cyber & Counsel

NAMIC
NATIONAL ASSOCIATION OF MUTUAL INSURANCE COMPANIES

317.875.5250 | [F] 317.879.8408
3601 Vincennes Road, Indianapolis, Indiana 46268

202.628.1558 | [F] 202.628.1601
20 F Street N.W., Suite 510 | Washington, D.C. 20001

NATIONAL ASSOCIATION OF INSURANCE COMMISSIONERS
CYBERSECURITY (H) WORKING GROUP

CYBERSECURITY EVENT RESPONSE PLAN (CERP)
OCTOBER 3, 2023 EXPOSURE DRAFT

NOVEMBER 3, 2023

On behalf of the National Association of Mutual Insurance Companies (NAMIC)[1] members, thank you for the opportunity to provide these comments on the Cybersecurity Event Response Plan (CERP) exposure draft materials circulated on October 3 (with additional confidentiality-related wording provided on October 13). NAMIC offered some initial input at the outset of the project (May 1). While some of the questions/concerns raised there were addressed, others were not and they continue to remain relevant.

As a general matter, the idea of having a ready Cybersecurity Event Response Plan to establish expectations is rational. And, in a number of important ways, sensible disclosures are set forth in the exposure draft. Yet, respectfully, the CERP is not ready for adoption without amendments being made and important matters being contemplated. These comments highlight crucial sets of issues in the context of the exposure draft:

- Effective **real uniformity** of regulatory cybersecurity event reporting is essential.
- **Workability** must be reliably built-into the CERP requirements.
- Avoid requests for over-sharing technical security details; observe **data minimization** principles.
- Strong **default confidentiality** is justified by seriousness and sensitivity of CERP's content.
- **Security** of CERP data – in transit and at rest – is crucial and indispensable.

[1] NAMIC Membership includes more than 1,500 member companies. The association supports regional and local mutual insurance companies on main streets across America and many of the country's largest national insurers. NAMIC member companies write $323 billion in annual premiums. Our members account for 67 percent of homeowners, 55 percent of automobile, and 32 percent of business insurance markets. Through our advocacy programs we promote public policy solutions that benefit NAMIC member companies and the policyholders they serve and foster greater understanding and recognition of the unique alignment of interests between management and policyholders of mutual companies.

Effective real uniformity of regulatory cybersecurity event reporting is essential.

Backdrop & Example Demonstrate Compelling Need for Uniformity

At the highest level, NAMIC supports efforts to make cyber incident reporting and response more uniform. The value of greater streamlining processes across jurisdictions is highlighted by the widespread MOVEit cyber incident (which occurred since the Working Group's initial request for comment on this matter in the Spring.) This may be a useful example case for industry and regulators to consider with respect to future CERP procedures and documentation – though insurance was far from the only industry hit (and it has been reported that several state governments were impacted as well). Among many learnings from that experience, MOVEit underscored the critical need for enhanced uniformity in cyber incident reporting and response requirements.

While on its face, it may appear that the NAIC's CERP process could meaningfully enhance uniformity, it may not because of the regulatory flexibility built into it. The NAIC's CERP does not meaningfully improve the very complex landscape that licensees must navigate quickly following a cyber incident. In short, **regulatory flexibility creates inconsistency**. Following a widespread incident, such as MOVEit, licensees are required to respond to numerous regulators operating on different timelines and using different procedures.

Expansion – States Going Beyond the Template

Unfortunately, there are places where the CERP introduces variability into what otherwise could be movement toward greater standardization and uniformity. For example, the **Understanding and Receiving Notifications Section** contains the following statement:

> States ***may also wish to consider gathering information*** to help the state understand the total exposure of the incident (e.g. total individuals/policyholders, total anticipated cost (if known), and information on cybersecurity coverage in place, etc.). Such information may allow the inquiring DOI to function as a lead state regulator to respond to the cybersecurity event, which may help minimize the total number of requests to licensees. (Emphasis added.)

While referencing a lead state regulator, there does not appear to be an indication that there would be a single lead state or that only one state would make such a request. It may be the case that this may function when there is one state involved, however there can be difficulties if multiple states are involved and each have their own inquiries. Because of these concerns, NAMIC urges either that the Working Group give more consideration to a strong explicit lead state approach or that the Working Group delete this paragraph which goes beyond the template and model to offer a suggestion as to what other information any number of states "may also wish" to gather.

Perpetuating the Current Reporting System vs.
Improving Reporting System through Increased Structure & Meaningful Value-Add

Again, consider the MOVEIt-related licensee reporting example and the overall current licensee reporting regulatory landscape. It involves a multi-pronged and substantial burden for licensees, delays responses, and can lead to greater harms for the consumer. In this response, licensees were responding to regulators from various states on differing timelines and who were requesting varying levels of information – all while responding to the incident. Such scenarios can slow the response to the incident, lead to duplicative notifications, create confusion for consumers, and potentially lead to additional harm.

When speed is critical following a cyber event, licensees should be able to dedicate finite resources toward fixing and mitigating the underlying vulnerability and customer communications — and not navigating a labyrinth of state-specific notification preferences. Indeed, an insurer reports that the burden of inconsistent obligations in a large scale incident is great due to competing deadlines and duplicative notifications – causing confusion an undue reputational harm.

Consider the Working Group's opportunity to improve the following current challenges:

- **Duplication/Inconsistency**: Inconsistent and sometimes duplicative notifications to consumers may unfairly harm insurers' reputations without meaningfully helping consumers. Inconsistent application of rules and variations in state specific rules may result in consumers receiving multiple notifications from a single insurer about a single incident. The Working Group could consider this problem and how to resolve it so it does not happen going forward. Further on consistency, as members express, it would be helpful to permit consumer notification requirements for licensees that are more consistent across industries. This may allow for a more common set of expectations and experiences for the consumer and allows insurers to focus on recovery and communication, not mandated variations in notice wording (or timelines outside of what is legislatively required). Even if not part of the current CERP project, please consider the value of this kind of effort in the future.

- **Multiple Regulatory Interests**: Continuing the point of consistency, as a general matter, several members shared the value of the Working Group' aligning with other most-prominent guidance on the matter because to the extent each Department varies greatly from other reporting information being sought, that introduces a high degree of onerous impact on companies that are likely also trying to eradicate a threat, respond to customers and the media, etc. Indeed, a member pointed to the potential value of allowing for coordinating with, or referencing referrals to the FBI Private Industry Notification (PIN) Network. Another member references the early 8-K filings under the SEC's Cyber Disclosure Rule and the reality of lighter initial detail where there is very short turnaround (such as 72 hours). Some financial institutions may also be looking to the FTC GLBA Safeguard Rule amendments addressing data breach notification.

As you can see, in addition to states, some licensees also need to look to federal and other sources as well. As we understand it, CISA may also currently be working through a new U.S. notification requirement for victims of malicious hacks. Even if not part of the current CERP project, consider possible future revisions to the CERP to account for the potential complexities from additional layers of regulatory interests.

- **Other Industries** & Disparity: It may cost more for insurance companies to respond to incidents that do not originate in our industry and equally impact other industries and the government. (This issue is raised less for resolution within the CERP than for awareness and potential consideration over the longer term.)

- **Leadership**: Streamlining, through regulator notification requirements, such as supporting a lead state approach, would simplify the process and help to address the complexity of post-incident reporting. In contrast to a situation in which a licensee is managing many regulatory communications with different states, consider the approach that allows for a licensee to be able to create one response that would be sufficient for situations involving regulators from multiple states (e.g., responding to the domiciliary state).

- **Posting** Policy: It is important that the ways Departments respond to an incident not increase litigation and class action risk for licensees more than other impacted industries. Publicly posting details of a licensee impacted by an incident may cause undue reputational harm to a licensee and create public distrust of the industry and licensee, especially in the case of third-party incidents. It is helpful when Departments refrain from publishing incident information that adds no meaningful consumer/industry protections (e.g., impacted licensee names). A policy approach of not making such postings could reduce potential misunderstanding and possible downstream impacts.

The Working Group's CERP deliverable provides the NAIC an opportunity to advance a more cohesive insurance regulatory notification framework and process on paper and in reality. NAMIC members encourage the NAIC to leverage this opportunity and to continue to work on this document until advancing consensus that will improve the processes post-incident (including post-cybercrime). Even beyond addressing the ways that the CERP document leaves room for inconsistencies with the amount of regulatory discretion written-into the draft, tangible ways the CERP could better serve all stakeholders, please consider the viability of possible additional components that would be helpful to licensees during this especially intense time of responding to an incident as well as to the working of the system overall.

The CERP draft references **regulators' possible wishes** to do/consider certain approaches in three different places. One instance – discussed above with regard to gathering additional information – would deviate from adding directional consistency. The other two places deal with communications.

- The **Forming a Team and Communicating with Consumers Section** states:

  Therefore, DOIs *may wish to have clear and defined protocols guiding external and internal communications* and to establish clear roles, responsibilities, and levels of decision-making authority to ensure a cohesive response to cybersecurity events at regulated entities.

- The **Understanding and Receiving Notifications Section** states:

  … DOIs *may wish to establish clear communication expectations* with the licensee to ensure updates provided are timely.

While it may be easier to finalize a document without coming to consensus and including some greater uniform reasonable standards (while still cognizant of the ways an incident may differ in complexity, facts, and circumstances, as acknowledged in the introductory paragraph of the Process for Responding to Cybersecurity Events Section) for communications-related expectations, regulators engaging in this area of cyber response preparedness in a way that develops reasonable consistency would benefit both the regulators and stakeholders when it comes time to dealing with an actual cybersecurity event (and especially one impacting residents across multiple jurisdictions).

NAMIC respectfully encourages the Working Group to address these kinds of opportunities.

Workability must be reliably built-into the CERP requirements.

Timing & Updates

A member conveys that as a general matter, the thirteen pieces of information contained on the template that licensees must provide insurance commissioners when a cybersecurity event occurs do not appear to be unreasonable overall and may offer regulators a route to providing a level of consistency. Yet, the CERP could be clearer around so obligations for updating and supplementing information.

With respect to **updates and timing**, compare the model and the CERP exposure draft:

- MDL-668 states: "… The Licensee shall have a continuing obligation to update and supplement initial and subsequent notifications to the Commissioner concerning the Cybersecurity Event."

- The CERP exposure draft **Understanding and Receiving Notifications Section** states: … "The licensee who notified the DOI of a breach is responsible for updating the data reported *as it becomes available*."

These differences raise several issues around **reasonability of expectations**:

- Immediacy & "As It Becomes Available": The model does not require a **real-time** rolling communication to each Department. Rather, it seems to allow a licensee to reasonably bundle updates, as it keeps the Commissioner informed of the details of a cybersecurity event. However, as currently drafted, the CERP would introduce a different expectation and may infer an even greater number of communications to each Department.

- Materiality: In looking at the list of items in Sec. 6(B) of MDL-668 and incorporated into the CERP Understanding and Receiving Notifications Section, it is appropriate that the regulators refer to obligations relating to "**material changes**." To do otherwise may imply a near impossible stream of communication and/or an uncertain regulatory environment. Indeed, the New York Department of Financial Services Final Adoption of the 2nd Amendment to 23 NYCRR 500, published earlier this week references that a "continuing obligation to update the superintendent with material changes or new information previously unavailable." (Sec. 500.17(a)(2).)

With these concerns in mind, NAMIC encourages the Working Group to change this wording along the lines of the following:

> "The licensee who notified the DOI of a breach ~~is responsible for updating~~ has a responsibility to update and supplement previous notifications to the Commissioner regarding material changes to previously provided information relating to the cybersecurity event as it relates to pieces of information from Section 6(B) of Model #668, to the extent possible ~~the data reported as it becomes available~~."

Further incorporating this materiality aspect elsewhere in the CERP aids all those involved.

While there is some acknowledgement toward the end of the **Understanding and Receiving Notifications Section** about it taking time to receive some information, members underscore the importance of this point overall as well as in the context of Departments asking additional questions and wanting all details immediately. They emphasize the importance of Departments exercising reasonable expectations on update reporting timing and detail. In addition to the "wish" aspect highlighted above, kindly consider inserting a reasonability aspect to this paragraph, such as:

> … The licensee who notified the DOI of a breach is responsible for updating the data reported as it becomes available. Where possible, DOIs should ~~may wish to~~ establish clear and reasonable communications with the licensee to ensure material updates provided are timely.

Process for Responding to Cybersecurity Events

Within the **Process for Responding to Cybersecurity Events Section** of the CERP exposure draft, there is reference to the "**determination.**" For clarity, is the "determination" being referred to intended to get at whether a "cybersecurity event" (as defined by law) has occurred or at the scope of the Department's engagement? Kindly consider wording to clarify this matter as it is an area where there could be multiple interpretations.

A member conveys that some of the questions posed in the CERP exposure draft's **Process for Responding to Cybersecurity Events Section** may only be relevant if the cybersecurity event happened within the licensee's infrastructure. If the event occurs with a **third-party** service provider (TPSP), questions may be irrelevant and/or create situations where an insurance company is acting as a "middle-person" between the regulator and the TPSP. It may be beneficial for the draft to identify questions that may/may not be relevant depending on which entity (the licensee itself or a TPSP) is the victim of the event.

Observe data minimization principles; avoid requests to over-share technical security details

There is no need for a regulator to collect **consumer level data** through this process. An explicit statement along these lines would be beneficial. The collection and storage of this level of information may raise another aspect to serious questions around data confidentiality and protection.

Whether in the **Understanding and Receiving Notifications Section** (overall details or with the possible additional discretionary requests) or under the **Process for Responding to Cybersecurity Events,** generally speaking we might describe a sense of an **inverse relationship** between the amount of information a licensee may feel comfortable providing and the robustness of data protection framework/assurances provided (including **confidentiality**). Data protection is discussed further below.

And certain **sensitive information** should be avoided; it should not be required to be reported. Specifically, information should not be transmitted regarding technical disclosures of security configuration and event detection. It is essential to avoid over-sharing that could expose a company to future breach and reverse-engineering. Over-sharing could occur in the 13 point incident notice, or in corrective action plan (see specific references below). Among the items that CERP should be clear about not including are things like:

- Vulnerable fields and configurations such as:
  - Specific File Transfer Protocol (FTP) parameters
  - Specific encryption standards
- Diagnostic evaluations
- Controls in place to mitigate security breach
- Corrective action plan

Within the **Understanding and Receiving Notices Section** there is a statement that the domestic regulator may also want to request additional information including a **corrective action plan**. However, it may provide the kind of road map for reverse engineering discussed above. NAMIC strongly urges that this be removed from the CERP exposure draft.

> If the licensee in question is the DOI's domestic licensee, it is the DOI's responsibility to ensure the company provides as much of this information as possible. ~~It may also be appropriate to request information in addition to the examples listed above, including a corrective action plan and status of consumer notifications, which can benefit the DOI's ongoing supervisory work.~~

Again though, data protection – even without collecting the most sensitive and vulnerability-creating information – is essential.

Strong default confidentiality is justified by the seriousness and sensitivity of the CERP content.

In its **Introduction Section**, the CERP exposure draft references MDL-668 and indicates that "If a state has made any changes in passing its version of Model #-668 or passed other regulations or legislation**, it will need to adjust the guidance herein accordingly**." [Kindly consider changing "will" to "may," as where language does not conflict having the uniformity of the CERP may be beneficial.] NAMIC would like to draw your attention to the way this statement is structured – it sets a default and then allows that adjustment may be necessary (though in the area of confidentiality less robust protection may therefore impact the regulators' ability to receive information from other states). **Default rules** are established in Section 8 of MDL-668 and CERP should be built to at least reflect these standards, while also being designed to allow other protections permitted under state law, including Freedom of Information Act and other privileges.

Based on the nature of information that is the focus of the CERP exposure draft, it must be clear that the 13 items within **Understand and Receiving Notifications Section** and the **Template** as well as any other requested information under one of those sections or under the **Process for Responding to Cybersecurity Events** (or elsewhere) must be held in confidence and not subject to **Freedom of Information Act** requests. This explicit approach would be consistent with the MDL-668 framework which serves as the foundation for the CERP. (See Sec. 8(A).) Again, it is essential that this be **built-into the CERP** given the nature of the discussion.

In addition to a basic FOIA exemption framework, the default approach should contemplate other appropriate privileges not needing to be asserted affirmatively – including but not limited to attorney client, compliance and audit privilege, trade secret, and others. If for some reason a state has received a request to disclose information and believes they may not be able to protect it, they should **inform** the licensee, so the licensee has the opportunity to review for potential rational for maintaining confidentiality as well as for potential risks of disclosure.

For example, item number 10 in the data list should prompt a recognition that the specifics of **internal review and audits** should be protected from regulatory disclosure and legal process under the compliance and audit privilege.

10	The results of any internal review identifying a lapse in either automated controls or internal procedures, or confirming that all automated controls or internal procedures were followed.

Also consider item number 11 relating to **remediation steps**. Without regulatory confidentiality, could expose the company to counter-productive litigation risk and future breach risk which is antithetical to the very purpose of regulator review of licensee handling of cybersecurity events.

11	Description of efforts being undertaken to remediate the situation which permitted the cybersecurity event to occur.

As you know, MDL-668 also contemplates possible examination and investigation. And regardless of whether a state has MDL-668 in place, it may have a market/financial regulation/analysis/conduct law that does afford appropriate confidentiality protections. To the extent necessary, a regulator could open a **targeted limited scope investigation/ examination** to provide explicit confidentiality protection to a licensee. This option should allow for the CERP to more incorporate conclusively necessary protection. To reiterate, this is especially compelling given the circumstances and the potential risks disclosure poses. Such a targeted effort should focus solely on the cybersecurity event; expansion of scope to unrelated issues could divert time and attention from the more urgent matters of the event.

Considering the concerns articulated above, NAMIC strongly suggests that the NAIC amend the confidentiality-related paragraphs in the **Process for Responding to Cybersecurity Events Section** to read something like the following:

> A state should treat any documents, materials, or other information in possession of the Department that are related to a cybersecurity event or related inquiry, investigation, or examination and that are furnished by a licensee as confidential and privileged under MDL-668, relevant examination/analysis laws, privileges, and other authority. As such, this information shall not be subject to any freedom of information or other open records law and shall not be subject to subpoena and shall not be subject to discovery or admissible in evidence in any private civil action. If a state cannot provide such confidentiality assurances or cannot protect certain information, it should disclose such limitations in writing to the licensee.

Similar to MDL-668, New York's Reg. 500.18 provides that any information provided related to a cybersecurity event is exempt from disclosure. Again, this overall default approach is straightforward and provides a clear set of expectations for all involved.

The final page of the draft CERP, Appendix A, offers a **Sample Template** for responding to DOI inquiries. While **NAMIC strongly urges the NAIC and state regulators to build-in strong uniform default confidentiality protection**, if that is not going to be done through the CERP, consider suggestions offered by different members as much lesser alternatives –

- Rather than a single template, having **separate forms** is pertinent to the extent submissions may be subject to public disclosure/FOIA requests.
- Directions on the form could be to clearly label any sections of responses with a **sensitivity label**—particularly for trade secret, privileged, or other confidential information such as vulnerabilities.

Security of CERP data – in transit and at rest – is crucial and indispensable.

As an overall matter, data protection is a serious matter. Whether it resides with licensees, state regulatory agencies, or the National Association of Insurance Commissioners (NAIC) (or is in transit between those types of entities), does not matter – standards and assurances around appropriate handling and protection of data should be straightforward and seamless.

Under **How to Receive Notifications and Acquire Required Information**, it is helpful see that the Working Group is considering some level of protections for **data in transit**. While there is overall reference to "reasonable security of the data in transit, commensurate with the sensitivity of the reported information," the specifics mentioned do not appear to fully meet this reasonability standard. Concerns are raised that the channels for filings and disclosures, including general email, may be unduly broad and insecure. Instead, regulators should incorporate stricter, more secure protocols, potentially including things like secure FTP, encrypted web services upload, and encrypted email. Also, as the Working Group knows, cyber technology/tools and security are continually evolving. To avoid the risk of getting out of date or becoming insecure, information security safeguards around receiving sensitive/confidential information should be assessed periodically (which would be consistent with the kinds of review required of licensees under MDL-668). With these concerns in mind, the Working Group might consider revisions along these lines:

> There are many options a DOI has for receiving notifications from licensees. To the extent consistent with ongoing review of secure protocols, options may include encrypted email, secure FTP, or encrypted web services upload. ~~an email inbox, an online form such as a PDF, or using a dedicated secure portal to complete an online form that stores that information in a database.~~ Before a cybersecurity event DOIs should take reasonable steps to ensure they have proper communication protocols and tools in place if the transmission of information is necessary. Communication channels established for event notification should provide reasonable security of the data in transit, commensurate with the sensitivity of the reported information. The security of communication protocols and channels should be reassessed periodically.

While the CERP exposure draft does reference data in transit, it does not appear to contain a corresponding section relating to **data at rest** – considerations should be given to **How to Store Required Information**. Given that confidential/sensitive information will be requested and then held, similar to the kinds of data protection considerations applying to licensees under MDL-668, regulators also should consider the protections they provide as well, taking into account good cyber hygiene practices ranging from authentication practices for accessing systems to encryption. The Working Group could review a number of possible sources beyond the NAIC's own model in developing such a section, including those from the security community and standards organizations (e.g., CISA, NIST, ISC2) and elsewhere. Indeed,

with regard to "sensitivity of the reported information," a member suggested consistency with the Confidential-Integrity-Availability Triad on configuration, storage and access to personal identifying and nonpublic financial information.

Further on the matter of storage, important **threshold questions** were posed in comments NAMIC submitted to the Working Group on May 1[2] which provided preliminary input regarding incident response. Those questions continue to appear relevant and NAMIC hopes to prompt internal regulator-NAIC discussions around the means by which greater volumes of sensitive/confidential information will be protected.

* * * * *

While completing the CERP, roughly as contained in the exposure draft, may address a Cybersecurity (H) Working Group charge, it appears to offer so much regulatory flexibility in implementation that it may circumvent addressing actual challenges regulated entities (also victims of cybercrimes) experience with inconsistent state notification requirements. Without driving toward greater consensus to improve consistency post-event, it seems that the NAIC may be missing an opportunity to make advancements beyond having a published CERP available. Further, the underlying inconsistent state notification requirements are not tackled. Finally, as mentioned, the confidentiality and security aspects of cyber event reporting are not incidental – they are core to the objectives of regulators, insurers, and consumers alike.

Before closing, NAMIC asks the Working Group to engage in an ongoing dialog with industry on efficiency (focusing on ways to improve consistency and streamline reporting) of cybersecurity reporting.

Kindly understand that NAMIC may seek to supplement comments as there is additional information as the process moves forward. NAMIC looks forward to working with the Cybersecurity (H) Working Group. Thank you.

[2] NAMIC response (May 1, 2023) to NAIC Cybersecurity (H) Working Group Request for Input, Incident Response (March 26, 2023)

Written Comments

Submitted by the

Center for Internet Security

November 3, 2023

Regarding the

Exposure Draft of the NAIC's Cybersecurity Event Response Plan (CERP)

Issued on

Wednesday, October 4, 2023

By the

Cybersecurity (H) Working Group

National Association of Insurance Commissioners

Introduction

Established in 2000 as an independent nonprofit organization, the Center for Internet Security's mission is to make the connected world a safer place by using open, collaborative deliberation processes to define, share, and sustain security best practices against cyber threats. These best practices represent the consensus opinion of experts from across the global security community and are freely available to all enterprises. CIS has over 20 years of success in developing, sharing, and sustaining security best practices, powered by a successful nonprofit business model. For example, CIS was instrumental in establishing the first public guidelines for security hardening of commercial IT systems (now known as CIS Benchmarks) when there was little online security leadership – and CIS is now the world's largest independent source of security configuration hardening.[1]

CIS operates both the Multi-State Information Sharing and Analysis Center ("MS-ISAC") and the Elections Infrastructure ISAC ("EI-ISAC"). Currently, these two ISACs provide cyber threat-sharing information and some cybersecurity defensive tools to all 56 states and territories and over 16,000 tribal and local government organizations.[2] Both ISACs work to improve the overall cybersecurity posture of the nation's SLTT governments through coordination, collaboration, cooperation, relevant and timely communication, and cybersecurity capabilities.

In addition, CIS is the home of the CIS Critical Security Controls,[3] the set of internationally-recognized, prescriptive, prioritized operational security practices that form the foundation of essential cyber hygiene--network defense that is demonstrated to prevent 80-90% of all known pervasive and dangerous cyberattacks. By design, the CIS Controls help implement the goals of the NIST framework by providing a roadmap for network operators to improve cybersecurity by identifying specific actions to be done in priority order based on the current state of the global cyber threat. What results is the clearest, most definitive blueprint of how to protect an organiza-

---

[1] For more information about the Center for Internet Security, please see: www.cisecurity.org

[2] For more information about the MS- and EI-ISACs, please see: https://www.cisecurity.org/ms-isac and https://www.cisecurity.org/ei-isac, respectively.

[3] For more information about the CIS Critical Security Controls, please see: https://www.cisecurity.org/controls

tion from cyberattacks. While the NIST Cybersecurity Framework ("NIST CSF") is the *what*--NIST defines the categories of cybersecurity and an organizational view of security risk management—the Controls are the *how*--the prioritized technical pathway to achieve the NIST goals. Moreover, the CIS Controls are specifically referenced in the NIST CSF as one of the tools to implement an effective cybersecurity program.[4]

CIS's ability to develop useful, real-world security practices like the CIS Controls is driven by our large-scale activity to gather feedback from worldwide users of our guidance and our nationwide, 24x7 mission operating the two ISACs (supporting all 56 states and territories and over 16,000 local and tribal government organizations).

Recommendations

"The primary goal of incident response is to identify threats on the enterprise, respond to them before they can spread, and remediate them before they can cause harm. Without understanding the full scope of an incident, how it happened, and what can be done to prevent it from happening again, defenders will just be in a perpetual "whack-a-mole" pattern."[5]

CIS commends the National Association of Insurance Commissions for seeking concrete ways to assist state departments of insurance in responding to cybersecurity incidents at a regulated insurance entity. We respectfully recommend for your consideration four cyber incident response documents:

(1) the Incident Response Commander Flowchart[6];

(2) the Incident Handling Commander Flowchart[7];

(3) the Incident Response Management Policy Template for CIS Control 17[8]; and

---

[4] NIST Cybersecurity Framework, Appendix A, page 20, and throughout the Framework Core (referred to as "CCS CSC" - Council on Cyber Security (the predecessor organization to CIS for managing the Critical Security Controls): https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[5] Center for Internet Security, Incident Response Management Policy Template for CIS Control 17; page 4: https://www.cisecurity.org/insights/white-papers/incident-response-policy-template-for-cis-control-17

[6] Attached to the transmittal of this comment at Appendix 1.

[7] Attached to the transmittal of this comment at Appendix 2.

[8] Attached to the transmittal of this comment at Appendix 3 and available at this link: https://www.cisecurity.org/insights/white-papers/incident-response-policy-template-for-cis-control-17

(4) the CIS Cyber Incident Checklist, intended for executives[9].

The first two documents resulted from efforts by the MS-ISAC's Business Resiliency Workbench Working Group. They are the current community-driven recommendations to help entities operationalize their IR plans. These were developed as a result of several key factors:

- Feedback from a poll question during an incident response webinar series where 97% of participants for that particular session said they would use CIRT for incident response *planning* if it was offered
- Individual outreach from SLTTs requesting assistance with their incident response plans (IRPs)
- Growing support within the SLTTs to assist others in identifying responsibilities/roles and helping to develop IRPs (i.e., crowdsourcing), and
- Identification of what seemed to be a trend of SLTTs developing IRPs that were not customized for operations. For example:
    - IRPs would be large, lengthy, complicated documents that would be too cumbersome to refer to at the time of action
    - IRP structure was lacking or inconsistent
    - Many templates were grabbed from the Internet and not customized to the organization
    - The IRPs often lacked clear roles and responsibilities with defined processes and workflows

The Business Resiliency Working Group that helped develop these two flowcharts currently consists of 34 members across CIS and our SLTT community including 5 critical infrastructure members, 2 states, 2 elections, 12 local governments (counties and below), 4 K-12, and 1 tribal member.

The third document, the *Incident Response Management Policy Template for CIS Control 17*, was developed as a support document for the CIS Critical Security Controls, the set of internationally-recognized, prescriptive, prioritized operational security practices that form the foundation of essential cyber hygiene--network defense that is demonstrated to prevent 80-90% of all

[9] Attached to the transmittal of this comment at Appendix 4.

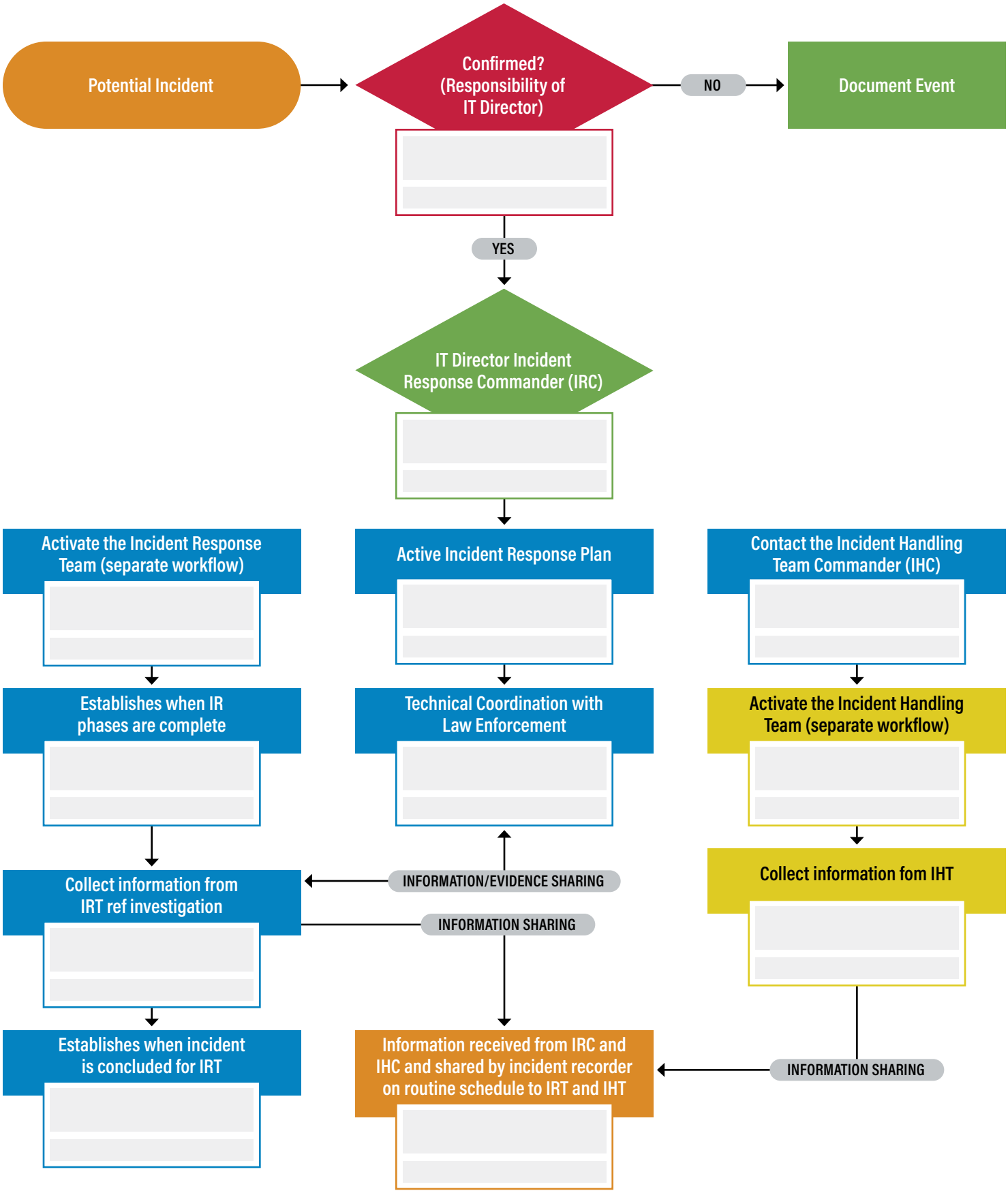
known pervasive and dangerous cyberattacks. The CIS Controls recommend multiple information security policies that an enterprise should have in place. This *Incident Response Policy* is meant as a starting point for organizations needing to draft their own policies and provides specific, high-level steps that should be part of any comprehensive incident response plan. Enterprises are encouraged to use this policy template in whole or in part. Obviously, there are multiple decision points and areas that must be tailored to your enterprise.

The fourth document is a cyber incident checklist designed for executives of both public and private sector organizations. The checklist identifies specific tasks that senior officials should focus on in three areas during a cyber incident: (1) establish reliable facts and a way to stay informed; (2) mobilize a response; and (3) communicate what you know.

We hope that these documents help inform the CERP's ability to support state departments of insurance in their response to notifications of cybersecurity events at regulated insurance entities. Please feel free to contact us if we can answer any questions that you might have or assist you in this important aspect of defending our nation.

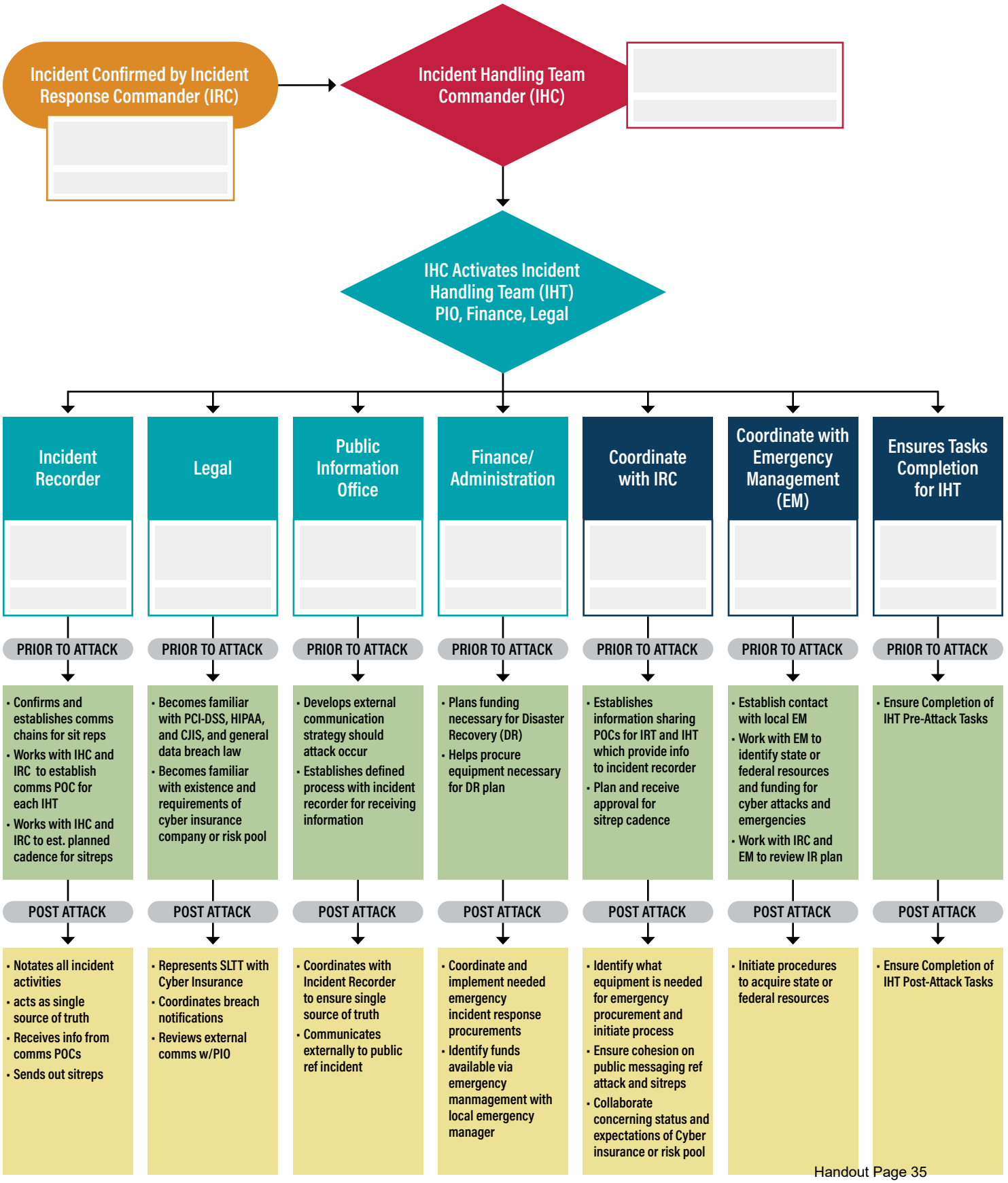
Incident Response Commander Flowchart

MS-ISAC®
Multi-State Information Sharing & Analysis Center®



Incident Handling Commander Flowchart

MS-ISAC®
Multi-State Information Sharing & Analysis Center®



Incident Response Policy Template

Critical Security Controls

March 2023

Contents

Contents **2**

Acknowledgments **3**

Introduction **4**

Purpose 4

Events vs Incidents 4

Scope 5

Incident Response Plan Lifecycle **6**

Incident Response Policy Template **8**

Purpose 8

Responsibility 8

Policy 8

Revision History **10**

Appendix A: Acronyms and Abbreviations **11**

Appendix B: Glossary **12**

Appendix C: Implementation Groups **14**

Appendix D: CIS Safeguards Mapping **15**

Appendix E: References and Resources **17**

Acknowledgments

The Center for Internet Security® (CIS®) would like to thank the many security experts who volunteer their time and talent to support the CIS Critical Security Controls® (CIS Controls®) and other CIS work. CIS products represent the effort of a veritable army of volunteers from across the industry, generously giving their time and talent in the name of a more secure online experience for everyone.

Editors:

Joshua M Franklin, CIS

Contributors:

Tony Krzyzewski, SAM for Compliance Ltd
Staffan Huslid, Truesec
Diego Bolatti, Information Systems Engineer, Universidad Tecnológica Nacional (Argentina)
Bryan Chou, CISSP, GSEC, GCED, GCIH
Bryan Ferguson
Gavin Willbond, SSS - IT Security Specialists
Ken Muir
Keala Asato
Jon Matthies
Chris Davis
Robin Regnier, CIS
Valecia Stocchetti, CIS

This work is licensed under a Creative Commons Attribution-Non Commercial-No Derivatives 4.0 International Public License. (The link can be found at https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode.)

To further clarify the Creative Commons license related to the CIS Controls® content, you are authorized to copy and redistribute the content as a framework for use by you, within your organization, and outside of your organization for non-commercial purposes only, provided that (i) appropriate credit is given to CIS, and (ii) a link to the license is provided. Additionally, if you remix, transform, or build upon the CIS Controls, you may not distribute the modified materials. Users of the CIS Controls framework are also required to refer to http://www.cisecurity.org/controls/ when referring to the CIS Controls in order to ensure that users are employing the most up-to-date guidance. Commercial use of the CIS Controls is subject to the prior approval of the Center for Internet Security, Inc. (CIS®).

Introduction

A comprehensive cybersecurity program includes protections, detections, response, and recovery capabilities. Often, the final two get overlooked in immature enterprises, or the response technique to compromised systems is just to re-image them to original state, and move on. The primary goal of incident response is to identify threats on the enterprise, respond to them before they can spread, and remediate them before they can cause harm. Without understanding the full scope of an incident, how it happened, and what can be done to prevent it from happening again, defenders will just be in a perpetual "whack-a-mole" pattern.

We cannot expect our protections to be effective 100% of the time. When an incident occurs, if an enterprise does not have a documented plan—even with good people—it is almost impossible to know the right investigative procedures, reporting, data collection, management responsibility, legal protocols, and communications strategy that will allow the enterprise to successfully understand, manage, and recover.

Along with detection, containment, and eradication, communication to stakeholders is key. If we are to reduce the probability of material impact due to a cyber event, the enterprise's leadership must know what potential impact there could be, so that they can help prioritize remediation or restoration decisions that best support the enterprise. These business decisions could be based on regulatory compliance, disclosure rules, service-level agreements with partners or customers, revenue, or mission impacts.

Dwell time from when an attack happens to when it is identified can be days, weeks, or months. The longer the attacker is in the enterprise's infrastructure, the more embedded they become and they will develop more ways to maintain persistent access for when they are eventually discovered. With the rise of ransomware, which is a stable moneymaker for attackers, this dwell time is critical, especially with modern tactics of stealing data before encrypting it for ransom.

Purpose

The CIS Critical Security Controls® (CIS Controls®) recommend multiple information security policies that an enterprise should have in place. This *Incident Response Policy* is meant as a "jumping off point" for organizations needing to draft their own policies, and provides specific, high-level steps that should be part of any comprehensive incident response plan. Enterprises are encouraged to use this policy template in whole or in part. With that said, there are multiple decision points and areas that must be tailored to your enterprise.

Events vs Incidents

There are many ways to define an incident. The authors of this document consider the following factors when defining an incident:

- An event or situation, either intentional or unintentional, internal to the enterprise or external,
- Caused by an individual, enterprise, nation state, or natural event that,
- Impacts an enterprise's ability to accomplish its mission (critically or otherwise), and
- This event may or may not lead to loss of data.

Examples of deliberate hacking incidents include attacks against Supermarket Chain Coop's and those affected by the SolarWinds Attacks. Incidents aren't always hacking-oriented as was the case with a French data center that was affected by fires, meaning natural disasters can also trigger the incident response plan. It can sometimes be difficult to interpret something as an *event* or an *incident*. NIST defines an *incident* as a "cybersecurity event that has been determined to have an impact on the organization prompting the need for response and recovery."[1] Some view an *event* as any occurrence that can be observed, verified, and documented, whereas an *incident* is one or more related events that negatively affect the company

[1] https://csrc.nist.gov/glossary/term/Cybersecurity_Incident

and/or impact its security posture. Sometimes one business unit within an enterprise will interpret an action as an event whereas another business unit will define it as an incident. This distinction matters, as an incident will trigger different enterprise responses, such as activating the incident response plan. Having clearly established definitions of events versus incident can be very beneficial for this reason. For example, an enterprise may determine that anytime leadership is actively involved in an event, it will be classified as an incident. Ultimately, this is a judgement call. Note that events can become incidents as more information is gathered.

Scope

This policy template is meant to supplement the CIS Controls v8. The policy statements included within this document can be used by all CIS Implementation Groups (IGs), but are geared towards Safeguards in Implementation Group 1 (IG1). Additional Safeguards from IG2 are included within this policy template, since they are commonly included as requirements from cyber insurance providers. These Safeguards are 17.4, 17.5, and 17.6. A mapping for Safeguards to the CIS Controls can be found in Appendix D. For more information on the CIS Implementation Groups, see Appendix C. Additionally, a glossary in Appendix B is provided for guidance on terminology used throughout the document. Future versions of this template may expand the scope to both Implementation Group 2 (IG2) Safeguards. IG2 and IG3 enterprises may feel the need to add sections that go beyond IG1, and are welcome to do so. Depending on an enterprise's sector or mission, other policy statements may also need to be added or removed. This is encouraged as this policy needs to be molded and fit to the enterprise's needs.

Incident Response Plan Lifecycle

This *Incident Response Policy Template* is divided into multiple sections based on usage patterns of assets within an enterprise. There are many ways to organize the incident response process. *The NIST Cybersecurity Framework (CSF)* provides one, as does *NIST 800-61 Revision 2: Computer Security Incident Handling Guide*. The lifecycle presented below in Figure 1 is an abstracted way to view the incident response process and house the policy statements provided by this document in an organized manner. High-level "steps" of the incident responses process are presented, followed by a detailed description of what each step entails.

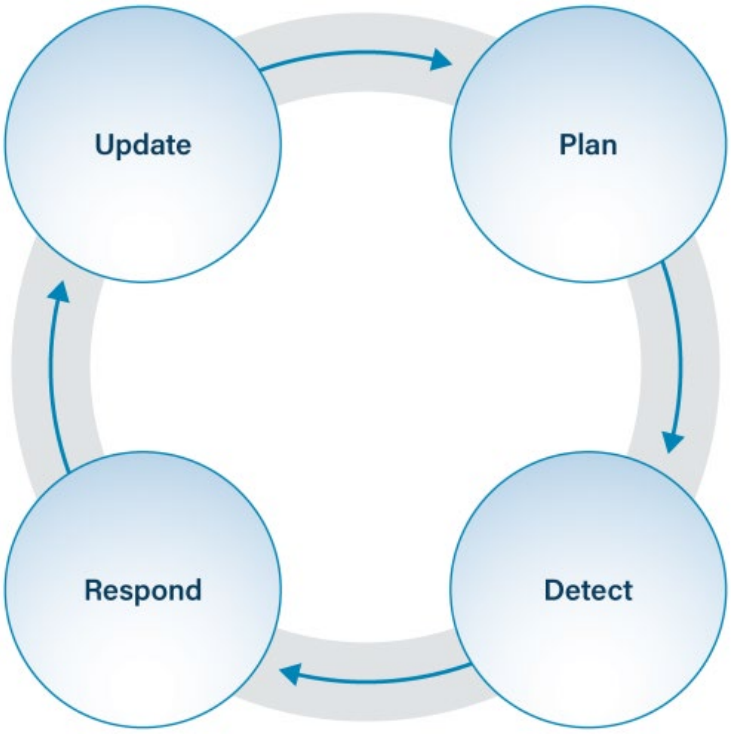


Figure 1. Incident Response Process

- **Plan** – Develop documentation for all procedures necessary to handle an incident.
- **Detect** – Monitor enterprise assets and analyze intelligence to understand if an incident has occurred.
- **Respond** – Activate the incident response plan to deal with an incident.
- **Update** – Understand which portions of the incident response plan have been effective or not, and update the plan accordingly.

Plan

When an incident occurs, the first step is to consult the incident response plan for the next steps that the enterprise should take. The plan should remain available in case enterprise systems are no longer functioning as intended; common methods include storing the plan on an external system or keeping a paper copy on hand. An incident will be a stressful time and this plan should provide step-by-step instructions that prevents guesswork during the heat of the moment. There are variety of incident response plans available online that enterprises can consult when writing their own plan. Plans will vary from enterprise to enterprise, but the level of detail will often be dictated by the maturity of the cybersecurity program. One of the most common aspects of an incident response plan is to name specific individuals to perform defined functions during this process. There will likely need to be someone who is responsible for the entire process, often the incident manager. Any

external support from third parties should also be named, which often includes contractors or technical organizations offering support. Detailed contact information should be provided for all individuals named in the plan. Once written, this plan will change over time as experience is gained, and the process gradually iterates to be in sync with the needs of the enterprise. Testing the plan via tabletop exercises is a great way to gain familiarity with the plan.

While larger enterprises may place procedures for responding to a natural disaster within a business continuity plan, smaller enterprises may place these policies within the incident response plan. Either approach is acceptable, and enterprises are encouraged to seek out how this is typically done in similar enterprises in their localities. Regulatory requirements may specifically note where these policies and procedures belong.

There is a need for a defined process for a user to report any identified event, or potential event. This process should be documented to facilitate clarity and ease of implementation. This is a separate plan or process from the Incident Response Plan. Users should be taught this process during the mandatory training for security awareness, therefore it must be easy to implement. The information should also be placed on internal intranet places and other logical places that would make the information readily available and accessible to all users.

Detect

Detecting if an incident occurred is difficult. Especially if the attack was subtle from advanced actors. To combat this, enterprises typically leverage a variety of methods to identify incidents such as data, anti-malware, and security awareness training. Data will often take the form of logs that must be analyzed. These logs may contain information to help you understand if an incident has occurred. Anti-malware tools such as endpoint detection and response (EDR) are tailor made for detecting these types of attacks. Finally, employees should be regularly trained on how to spot and report incidents. This means that IT must monitor employee reports of computer incidents and actively investigate such reports.

Respond

Once an incident has been reported or detected, IT, or the business units charged with security, must activate the incident response plan as developed in the planning phase. This response also begins the recovery process. The response team will often be composed of internal and external users all working together to carry out the incident response plan. It's common for smaller enterprises to contact any contractors helping to manage its IT infrastructure or any state/federal government entities offering free or low-cost services. Ultimately, the individual specified in the incident response plan as the incident manager is charged with ensuring the incident has been properly managed and is following established standard operating procedures (SOPs). It's best practice for the incident manager to be an individual trained in incident response with excellent communication skills, the capacity to prioritize the incident. This individual must have the authority to communicate business impacts with external organizations such as lawyers, regulators, cyber insurance companies, local cyber incident response teams (CIRT) and potentially law enforcement. Generally, this is not a senior executive; but this is not always practical with smaller entities. External incident response expertise may be required. This individual will also be responsible for making the determination that the incident has come to a conclusion.

Update

The update phase of this lifecycle ensures that the incident response plan and process is gradually improving from the experiences of recent incidents, tabletop exercises, and scheduled regular review. Lessons learned from recent incidents should be discussed with the individuals involved in the incident response process. Appropriate changes to the incident response plan based on recent incidents should be made, alongside the standard operating procedures. Where applicable, communicate and train staff on changes to the IR plan. During the incident response process, it's common for data to be collected and used to help guide actions of all involved. These collected data artifacts should be archived or deleted in a manner consistent with the *Data Management Policy* and documented it in the custodial chain of evidence if appropriate.

Incident Response Policy Template

Purpose

Incident response includes planning for and actively managing incidents that can prevent an enterprise from leveraging its assets to meet its goals. Most commonly this takes the form of unauthorized access into a computer system, physical security intrusions, or if a natural disaster occurs. The *Incident Response Policy* provides the processes and procedures for ensuring incidents are properly handled with as little impact to the enterprise as possible, and to begin the recovery plan. This policy applies to all departments and all assets connected to the enterprise network.

Responsibility

- The IT business unit is responsible for managing all incident response functions.
    - While all IT staff are required to follow the written incident response plan, real world deviations are expected and must be handled gracefully. Third-party organizations involved in the incident response process must be managed by the incident manager.
- Users are responsible for reporting incidents that they are aware of to the appropriate business unit or personnel as specified in the incident reporting process. Users are responsible for attending training for recognizing and reporting incidents within the enterprise.

Policy

Plan

1. IT must develop and maintain a written incident response plan.
    a. This process must be documented and approved.
    b. This plan must include a process for responding to incidents.
    c. At a minimum, the incident response process must be reviewed on an annual basis or following significant changes within the enterprise.
        a. This review may also occur following an incident or tabletop exercise.
    d. An incident manager and backup incident manager must be specifically identified by name within the plan.
        a. If an external party is the incident manager, then one internal individual must be specified to oversee the response process.
        b. Contact information must be recorded in the incident response plan.
    e. Any parties that need to be made aware of a security incident must be documented.
    f. The plan must address any regulatory or other compliance requirements.
    g. The plan must address communications.
2. IT must develop and maintain a written process for users to report incidents.
    a. This process must include approved methods for reporting incidents including:
        a. Primary and secondary methods for reporting.
        b. Specific recipients to receive incident reports.
        c. Any minimum information needed.
        d. Timeframes for reporting incidents.
    b. At a minimum, the incident reporting process must be reviewed on an annual basis or following significant changes within the enterprise.

Detect

There are no IG1 safeguards that support this portion of the incident response process.

Respond

There are no IG1 safeguards that support this portion of the incident response process.

Update

1. At a minimum, the incident response and reporting processes must be reviewed on an annual basis or following significant changes within the enterprise.

Revision History

Each time this document is updated, this table should be updated.

Version	Revision Date	Revision Description	Name

Appendix A: Acronyms and Abbreviations

CIS	Center for Internet Security
CIS Controls	Center for Internet Security Critical Security Controls
CIRT	Cyber Incident Response Team
COTS	Commercial-off-the-shelf
CSF	Cybersecurity Framework
EDR	Endpoint Detection and Response
IG	Implementation Group
IR	Incident Response
ISAC	Information Sharing and Analysis Center
IT	Information Technology
OSINT	Open-source intelligence
SOP	Standard Operating Procedure

Appendix B: Glossary

Asset	Anything that has value to an organization, including, but not limited to, another organization, person, computing device, information technology (IT) system, IT network, IT circuit, software (both an installed instance and a physical instance), virtual computing platform (common in cloud and virtualized computing), and related hardware (e.g., locks, cabinets, keyboards). Source: Asset(s) - Glossary | CSRC (nist.gov)
Cloud environment	A virtualized environment that provides convenient, on-demand network access to a shared pool of configurable resources such as network, computing, storage, applications, and services. There are five essential characteristics to a cloud environment: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. Some services offered through cloud environments include Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).
Enterprise assets	Assets with the potential to store or process data. For the purpose of this document, enterprise assets include end-user devices, network devices, non-computing/Internet of Things (IoT) devices, and servers in virtual, cloud-based, and physical environments. Source: CIS Controls v8
Network devices	Electronic devices required for communication and interaction between devices on a computer network. Network devices include wireless access points, firewalls, physical/virtual gateways, routers, and switches. These devices consist of physical hardware as well as virtual and cloud-based devices. For the purpose of this document, network devices are a subset of enterprise assets. Source: CIS Controls v8
Physical environment	Physical hardware parts that make up a network, including cables and routers. The hardware is required for communication and interaction between devices on a network. Source: CIS Controls v8
Portable end-user devices	Transportable, end-user devices that have the capability to wirelessly connect to a network. For the purpose of this document, portable end-user devices can include laptops and mobile devices such as smartphones and tablets, all of which are a subset of enterprise assets. Source: CIS Controls v8
User	Employees (both on-site and remote), third-party vendors, contractors, service providers, consultants, or any other user that operates an enterprise asset. Source: CIS

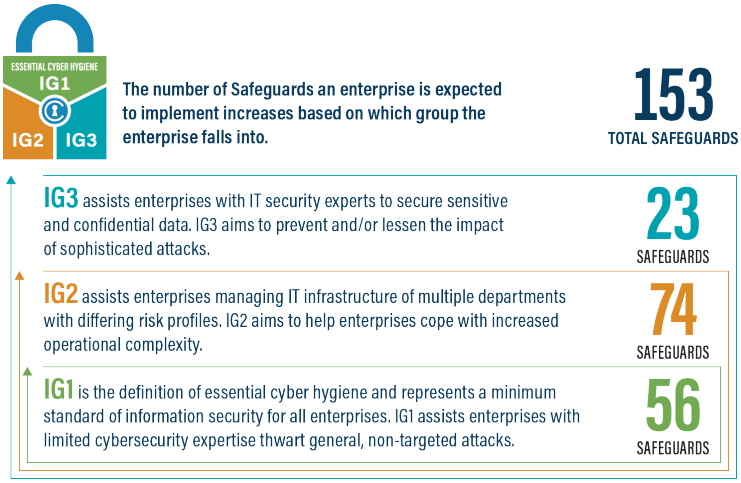
Virtual environment	Simulates hardware to allow a software environment to run without the need to use a lot of actual hardware. Virtualized environments are used to make a small number of resources act as many with plenty of processing, memory, storage, and network capacity. Virtualization is a fundamental technology that allows cloud computing to work. Source: CIS Controls v8

Appendix C: Implementation Groups

As a part of our most recent version of the CIS Controls, v8, we created Implementation Groups (IGs) to provide granularity and some explicit structure to the different realities faced by enterprises of varied sizes.

IG1

An IG1 enterprise is small- to medium-sized with limited IT and cybersecurity expertise to dedicate towards protecting IT assets and personnel. The principal concern of these enterprises is to keep the business operational, as they have a limited tolerance for downtime. The sensitivity of the data that they are trying to protect is low and principally surrounds employee and financial information. Safeguards selected for IG1 should be implementable with limited cybersecurity expertise and aimed to thwart general, non-targeted attacks. These Safeguards will also typically be designed to work in conjunction with small or home office commercial off-the-shelf (COTS) hardware and software.



IG2

An IG2 enterprise employs individuals responsible for managing and protecting IT infrastructure. These enterprises support multiple departments with differing risk profiles based on job function and mission. Small enterprise units may have regulatory compliance burdens. IG2 enterprises often store and process sensitive client or enterprise information, and they can withstand short interruptions of service. A major concern is loss of public confidence if a breach occurs. Safeguards selected for IG2 help security teams cope with increased operational complexity. Some Safeguards will depend on enterprise-grade technology and specialized expertise to properly install and configure.

IG3

An IG3 enterprise employs security experts that specialize in the different facets of cybersecurity (e.g., risk management, penetration testing, application security). IG3 assets and data contain sensitive information or functions that are subject to regulatory and compliance oversight. An IG3 enterprise must address availability of services and the confidentiality and integrity of sensitive data. Successful attacks can cause significant harm to the public welfare. Safeguards selected for IG3 must abate targeted attacks from a sophisticated adversary and reduce the impact of zero-day attacks.

If you would like to know more about the Implementation Groups and how they pertain to enterprises of all sizes, there are many resources that explore the Implementation Groups and the CIS Controls in general on our website at https://www.cisecurity.org/controls/cis-controls-list/.

Appendix D: CIS Safeguards Mapping

CIS Controls & Safeguards Covered by this Policy

This policy helps to bolster IG1 Safeguards in CIS Control 17: *Incident Response Management*. Table 1 shows which IG1 Safeguards are covered by this policy as written.

Table 1 - Safeguards covered by IG1

CIS Control	Policy Statement	CIS Safeguard Title	CIS Safeguard Description
17.1	Plan 1d	Designate Personnel to Manage Incident Handling	Designate one key person, and at least one backup, who will manage the enterprise's incident handling process. Management personnel are responsible for the coordination and documentation of incident response and recovery efforts and can consist of employees internal to the enterprise, third-party vendors, or a hybrid approach. If using a third-party vendor, designate at least one person internal to the enterprise to oversee any third-party work. Review annually, or when significant enterprise changes occur that could impact this Safeguard.
17.2	Plan 1db	Establish and Maintain Contact Information for Reporting Security Incidents	Establish and maintain contact information for parties that need to be informed of security incidents. Contacts may include internal staff, third-party vendors, law enforcement, cyber insurance providers, relevant government agencies, Information Sharing and Analysis Center (ISAC) partners, or other stakeholders. Verify contacts annually to ensure that information is up-to-date.
17.3	Plan 2	Establish and Maintain an Enterprise Process for Reporting Incidents	Establish and maintain an enterprise process for the workforce to report security incidents. The process includes reporting timeframe, personnel to report to, mechanism for reporting, and the minimum information to be reported. Ensure the process is publicly available to all of the workforce. Review annually, or when significant enterprise changes occur that could impact this Safeguard.
17.4	Plan 1	Establish and Maintain an Incident Response Process	Establish and maintain an incident response process that addresses roles and responsibilities, compliance requirements, and a communication plan. Review annually, or when significant enterprise changes occur that could impact this Safeguard.
17.5	Plan 1de	Assign Key Roles and Responsibilities	Assign key roles and responsibilities for incident response, including staff from legal, IT, information security, facilities, public relations, human resources, incident responders, and analysts, as applicable. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

CIS Control	Policy Statement	CIS Safeguard Title	CIS Safeguard Description
17.6	Plan 1g	Define Mechanisms for Communicating During Incident Response	Determine which primary and secondary mechanisms will be used to communicate and report during a security incident. Mechanisms can include phone calls, emails, or letters. Keep in mind that certain mechanisms, such as emails, can be affected during a security incident. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

Appendix E: References and Resources

Center for Internet Security®
https://www.cisecurity.org/

CIS Critical Security Controls®
https://www.cisecurity.org/controls/

Council of Registered Security Testers (CREST) Cyber Security Incident Response Guide
https://www.crest-approved.org/wp-content/uploads/2014/11/CSIR-Procurement-Guide.pdf

NIST SP 800-61 Rev. 2 Computer Security Incident Handling Guide
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

NIST SP 800-184 Guide for Cybersecurity Event Recovery
https://csrc.nist.gov/publications/detail/sp/800-184/final

MS-ISAC® and EI-ISAC® Service: Cyber Incident Response Team (CIRT)
SLTT governments can report incidents to the MS-ISAC Call 866-787-4722 or email soc@cisecurity.org for assistance from the MS-ISAC/EI-ISAC Security Operations Center (SOC) and Cyber Incident Response Team (CIRT)

Cyber Incident Checklist

Center for Internet Security®

MS-ISAC®
Multi-State Information Sharing & Analysis Center®

Elections Infrastructure ISAC®

1 Establish Reliable Facts and a Way to Stay Informed

- ◯ **Who** is reporting the problem? How did they become aware?
- ◯ **What** do we know so far about what happened?
  - What networks/systems are affected?
  - What data/information was compromised (e.g., stolen, deleted, altered)?
- ◯ **When** did the breach occur?
  - When did we find out about it?
  - When did we begin to do some thing about it?
  - When will we know the full scope of the problem?
  - When do we estimate that the problem will be remediated?
- ◯ **Where** did the breach occur (what office, activity, locale, etc.)?
- ◯ **How** much do we know, with certainty, about how the breach occurred? The source of the attack?
- ◯ **How** will we stay informed of efforts to remediate the breach and restore normal service?

2 Mobilize a Response

- ◯ Who has the lead in directing operational response efforts? What role will your office play?
- ◯ Has the MS- or EI-ISAC been notified (+1 866.787.4722)?
- ◯ Who else should be notified at this point (e.g., citizens, business and industry, other state, local, federal officials)?
- ◯ Has law enforcement been notified?
- ◯ What expertise is on hand to work the problem? What additional help do you need? Who will provide it?
- ◯ What measures are needed to secure the networks/systems from further exploitation?
- ◯ What additional steps are needed to secure data holdings?
- ◯ How will the remediation efforts to limit/repair the damage and restore normal services be prioritized?
- ◯ What special notifications should be prepared for victims?
- ◯ What other actions do your breach notification laws require?
- ◯ What are the legal implications of the incident?

3 Communicate What You Know

- ◯ Here, as elsewhere, bad news does not get better with age, but remember the general rule that the first report is always wrong.
- ◯ Release your initial public statement as soon as you have a reasonable command of the problem and can explain what you are doing about it.
- ◯ Describe what you know so far about what happened and what is being done to correct it.
- ◯ Be prepared to explain the pre-existing cybersecurity posture and the measures that were in place to prevent events of this kind.
- ◯ Be prepared to explain the steps you will take to prevent future unauthorized intrusions. Start with basic cyber hygiene and the CIS Controls.
- ◯ Establish a regular cadence of updates for victims, media, and other stakeholders—including your own workforce.

Headquarters
31 Tech Valley Drive
East Greenbush, NY 12061
+1 518.266.3460

www.cisecurity.org

Need Help?
Call or email the MS- or EI-ISAC
+1 866.787.4722 (24 hours)

soc@cisecurity.org

elections@cisecurity.org

How do I join?
Complete our registration form at

MS-ISAC
https://learn.cisecurity.org/ms-isac-registration

EI-ISAC
https://learn.cisecurity.org/ei-isac-registration

Receive and Update on the National Institute of Standards and Technology (NIST) Cybersecurity Framework

Journey to the NIST Cybersecurity Framework 2.0

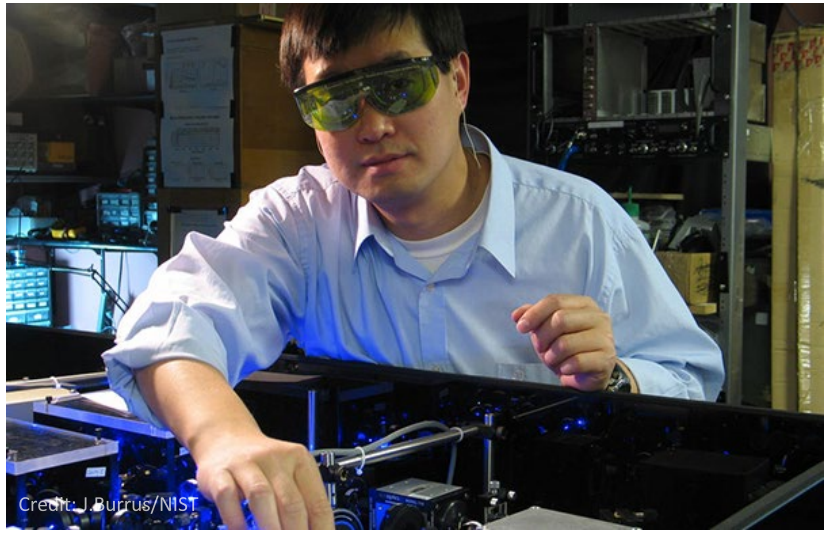
National Association of Insurance Commissioners (NAIC)
November 2023

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Mission

To promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life







NIST AT A GLANCE
Industry's National Laboratory

3,400+
FEDERAL EMPLOYEES

5
NOBEL PRIZES

2 CAMPUSES
GAITHERSBURG, MD [HQ]
BOULDER, CO

3,500+
ASSOCIATES

10
COLLABORATIVE INSTITUTES

400+
BUSINESSES USING NIST FACILITIES

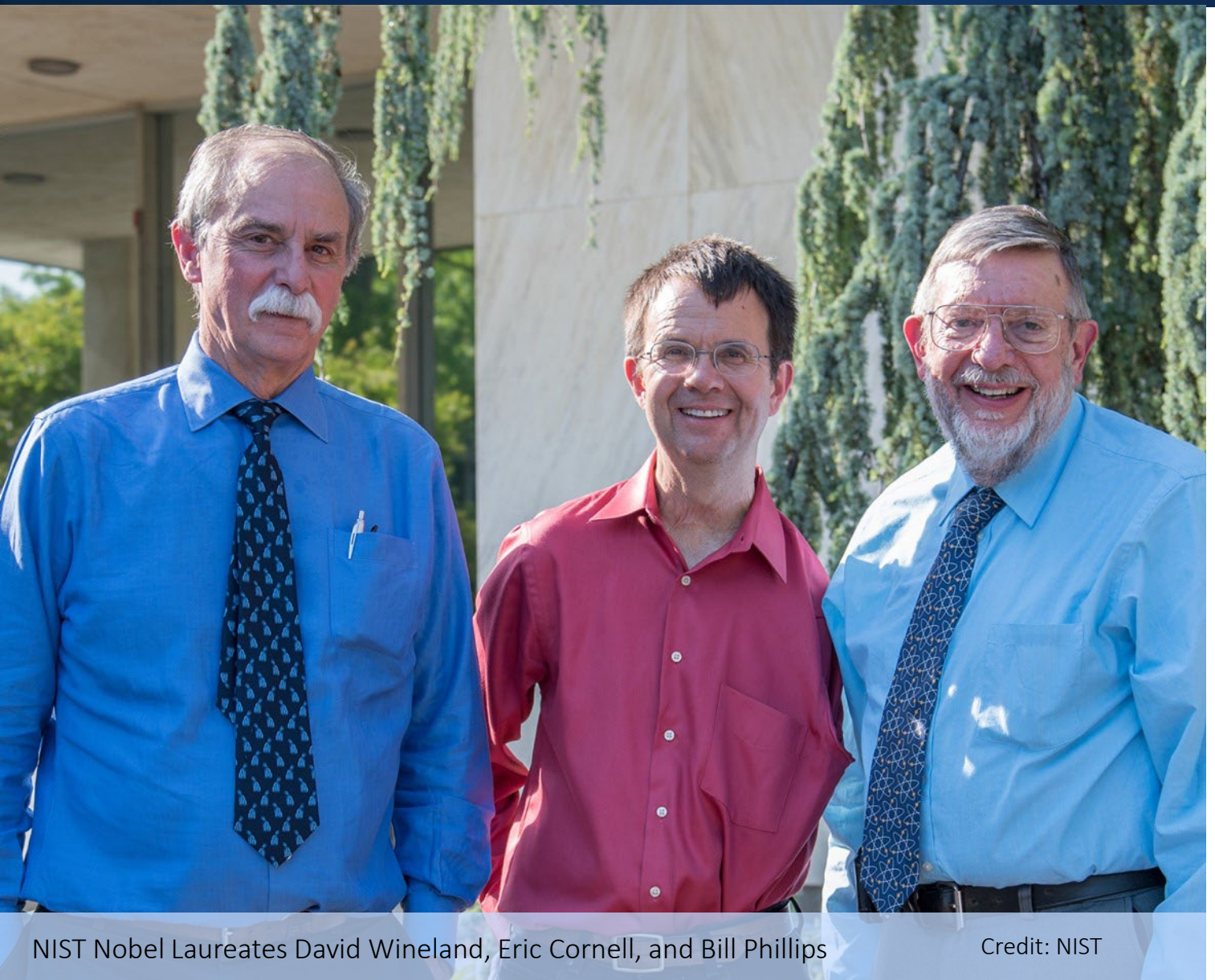
ManufacturingUSA

16
NATL OFFICE FOR MANUFACTURING INSTITUTES

51
MANUFACTURING EXTENSION PARTNERSHIP CENTERS

U.S. BALDRIGE PERFORMANCE EXCELLENCE PROGRAM

NIST's Biggest Strength: Our Reputation



NIST Nobel Laureates David Wineland, Eric Cornell, and Bill Phillips

Credit: NIST

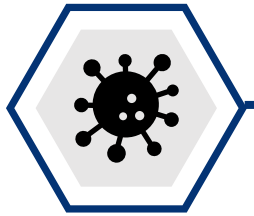
- Technical excellence
- Integrity
- Uncompromising
- Rigorous
- Unbiased
- Industry focused
- Non-regulatory

Critical & Emerging Technologies



ARTIFICIAL INTELLIGENCE

Transparent, trustworthy AI and machine learning



BIOTECHNOLOGY

And engineering biology to impact the health, agricultural, and industrial sectors



CYBERSECURITY AND PRIVACY

To enable the development and deployment of emerging technologies



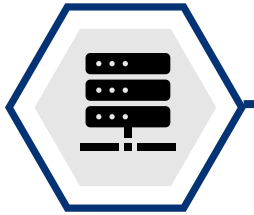
ADVANCED COMMUNICATIONS

(5G and beyond) and wireless technologies



ENERGY TECHNOLOGIES

Generation, storage, distribution, and secure, climate-friendly, efficient utilization of energy



QUANTUM INFORMATION SCIENCE

Leveraging quantum mechanics for the storage, transmission, manipulation, computing, or measurement of information

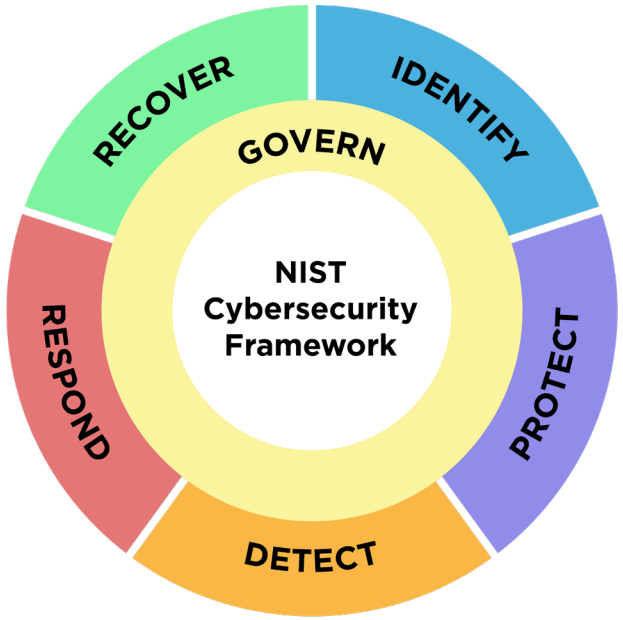
CSF Update | Journey to CSF 2.0

- **NIST is updating the Cybersecurity Framework** to address the evolving cybersecurity risk and standards landscape and make it easier for organizations to address risks. NIST is actively relying on and seeking diverse stakeholder feedback in the update process.



Ways to engage: www.nist.gov/cyberframework

JUST RELEASED | Draft CSF 2.0



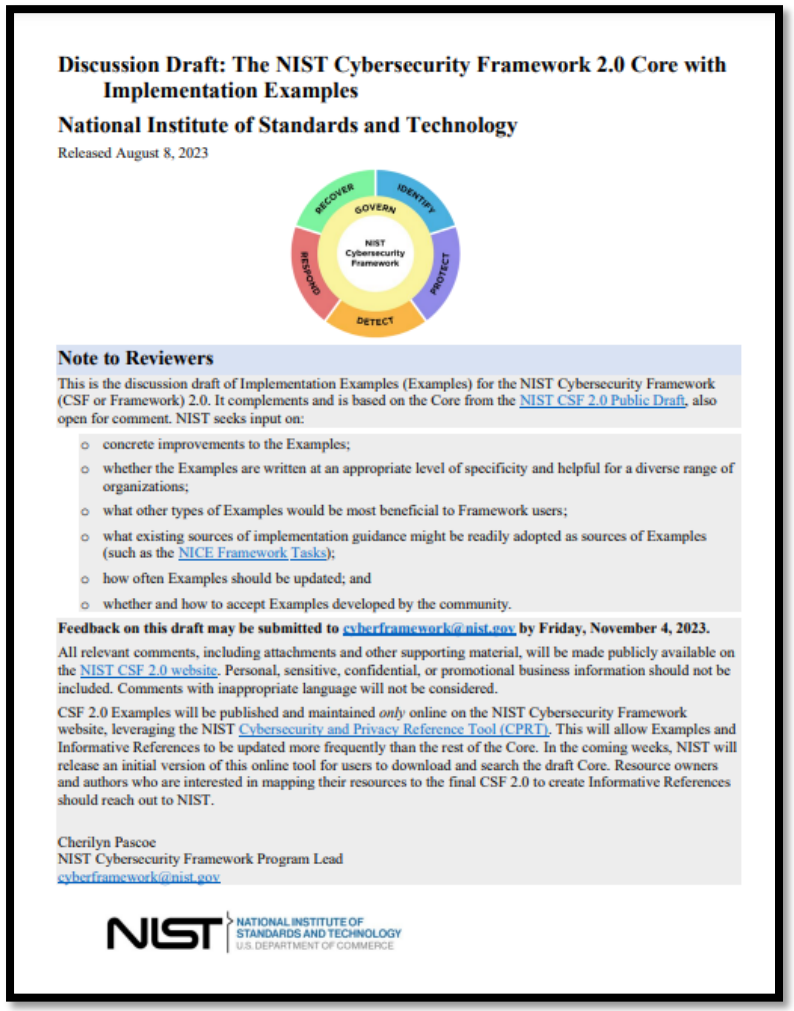
This newly released draft represents a major update to the CSF, which was first released in 2014.

Key Updates:

- Reflects changes in the cybersecurity landscape (risks, technologies, standard changes)
- Makes it easier to put the CSF into practice for all organizations through additional guidance on implementing the CSF
- An expanded scope beyond critical infrastructure.
- The addition of a sixth function, Govern.
- Additional coverage of supply chain security.

Comments on the Draft Core may be sent to cyberframework@nist.gov by November 4, 2023.

CSF 2.0 Discussion Draft
Revised Core with Implementation Examples



Discussion Draft: The NIST Cybersecurity Framework 2.0 Core with Implementation Examples

National Institute of Standards and Technology

Released August 8, 2023

Note to Reviewers

This is the discussion draft of Implementation Examples (Examples) for the NIST Cybersecurity Framework (CSF or Framework) 2.0. It complements and is based on the Core from the NIST CSF 2.0 Public Draft, also open for comment. NIST seeks input on:

- concrete improvements to the Examples;
- whether the Examples are written at an appropriate level of specificity and helpful for a diverse range of organizations;
- what other types of Examples would be most beneficial to Framework users;
- what existing sources of implementation guidance might be readily adopted as sources of Examples (such as the NICE Framework Tasks);
- how often Examples should be updated; and
- whether and how to accept Examples developed by the community.

Feedback on this draft may be submitted to cyberframework@nist.gov by Friday, November 4, 2023.

All relevant comments, including attachments and other supporting material, will be made publicly available on the NIST CSF 2.0 website. Personal, sensitive, confidential, or promotional business information should not be included. Comments with inappropriate language will not be considered.

CSF 2.0 Examples will be published and maintained *only* online on the NIST Cybersecurity Framework website, leveraging the NIST Cybersecurity and Privacy Reference Tool (CPRT). This will allow Examples and Informative References to be updated more frequently than the rest of the Core. In the coming weeks, NIST will release an initial version of this online tool for users to download and search the draft Core. Resource owners and authors who are interested in mapping their resources to the final CSF 2.0 to create Informative References should reach out to NIST.

Cherilyn Pascoe
NIST Cybersecurity Framework Program Lead
cyberframework@nist.gov

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

nist.gov/document/discussion-draft-nist-cybersecurity-framework-20-core-implementation-examples

The following are links to each of the CSF 2.0 Function tables with Implementation Examples:

Table 1. **GOVERN (GV): Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy**
Table 2. **IDENTIFY (ID): Help determine the current cybersecurity risk to the organization**
Table 3. **PROTECT (PR): Use safeguards to prevent or reduce cybersecurity risk**
Table 4. **DETECT (DE): Find and analyze possible cybersecurity attacks and compromises**
Table 5. **RESPOND (RS): Take action regarding a detected cybersecurity incident**
Table 6. **RECOVER (RC): Restore assets and operations that were impacted by a cybersecurity incident**

Comments on the Discussion Draft may be sent to cyberframework@nist.gov by November 4, 2023.

Implementation Examples and Informative References

Category	Subcategory	Implementation Examples	Informative References
		applicable cybersecurity risks, and integrate them into organizational policies and applicable third-party agreements **Ex7:** Internally communicate cybersecurity supply chain risk management roles and responsibilities for third parties **Ex8:** Establish rules and protocols for information sharing and reporting processes between the organization and its suppliers	
	GV.SC-03: Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes (formerly ID.SC-02)	**Ex1:** Identify areas of alignment and overlap with cybersecurity and enterprise risk management **Ex2:** Establish integrated control sets for cybersecurity risk management and cybersecurity supply chain risk management **Ex3:** Integrate cybersecurity supply chain risk management into improvement processes **Ex4:** Escalate material cybersecurity risks in supply chains to senior management, and address them at the enterprise risk management level	
	GV.SC-04: Suppliers are known and prioritized by criticality	**Ex1:** Develop criteria for supplier criticality based on, for example, the sensitivity of data processed or possessed by suppliers, the degree of access to the organization's systems, and the importance of the products or services to the organization's mission **Ex2:** Keep a record of all suppliers, and prioritize suppliers based on the criticality criteria	
	GV.SC-05: Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties (formerly ID.SC-03)	**Ex1:** Establish security requirements for suppliers, products, and services commensurate with their criticality level and potential impact if compromised **Ex2:** Include all cybersecurity and supply chain requirements that third parties must follow and how compliance with the requirements may be verified in default contractual language **Ex3:** Define the rules and protocols for information sharing between the organization and its suppliers and sub-tier suppliers in contracts **Ex4:** Manage risk by including security requirements in contracts based on their criticality and potential impact if compromised	

Governance Function: C-SCRM Category

GV.SC-01: A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders (formerly ID.SC-01)

GV.SC-02: Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally (formerly ID.AM-06)

GV.SC-03: Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes (formerly ID.SC-02

GV.SC-04: Suppliers are known and prioritized by criticality

GV.SC-05: Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties (formerly ID.SC-03)

Governance Function: C-SCRM Category

GV.SC-06: Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships

GV.SC-07: The risks posed by a supplier, their products and services, and other third parties are identified, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship (formerly ID.SC-02, ID.SC-04)

GV.SC-08: Relevant suppliers and other third parties are included in incident planning, response, and recovery activities (formerly ID.SC-05)

GV.SC-09: Supply chain security practices are integrated into cybersecurity and enterprise risk management programs, and their performance is monitored throughout the technology product and service life cycle

GV.SC-10: Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclusion of a partnership or service agreement

CSF 2.0 Next Steps



- **Public workshops and events**
  - Third and final CSF 2.0 Workshop → September 19-20 at the NIST NCCoE.
  - Find recordings of CSF Workshop #1 (August 2022) and #2 (February 2023) online.
- **Comment on drafts**
  - Provide comments on the Draft CSF 2.0 and the Discussion Draft by November 4, 2023 (all prior comments received can be found online).
- **Continuing to seek and develop CSF resources, success stories, and mappings to other frameworks and standards.**

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

STAY IN TOUCH

CONTACT US

NIST.gov

@NISTcyber

Receive an Update on Federal Activities Related to Cybersecurity

Discuss Any Other Matters