

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).

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.

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.

SharePoint/NAIC Support Staff Hub/Member Meetings/H CMTE/2023_Spring/WG-Cybersecurity/Cyber-WG-Minutes030723.docx

Cybersecurity Event Response Plan (CERP)

Introduction

The Cybersecurity Event Response Plan (CERP) is intended to support Departments of Insurance (DOIs) in their response following notification or otherwise becoming aware of a cybersecurity event at a regulated insurance entity (licensee).

This guidance follows the definitions and sections of the NAIC Insurance Data Security Model Law (#668), specifically the process detailed in Section 6, “Notification of a Cybersecurity Event.” If a state has made any changes in passing its version of Model #668 or passed other regulations or legislation, it may need to adjust the guidance herein accordingly.

Furthermore, the CERP is focused on primary actions and considerations, and it should be tailored to suit a DOI’s needs. Additionally, DOIs that implement a CERP, whether leveraging the guidance of the NAIC or not, need to ensure that CERP roles and expectations are widely understood throughout the DOI. The effectiveness of a DOI’s response to a cybersecurity event will improve if roles are clearly defined and understood. An effective CERP may assist DOIs in facilitating communication between stakeholders. In the wake of a cybersecurity event, licensees will have to address many reporting requirements either related to state or federal laws. Therefore, the CERP is written to assist a DOI’s process to respond to a licensee’s cybersecurity event in a way that allows the DOI to consistently gather as much required information as possible without unduly burdening the licensee. Therefore, the CERP is also written to support and encourage the use of the Lead State concept where possible and appropriate.

Scope

This response plan does not specifically address which events must be reported, as cybersecurity laws and regulations vary from state to state. DOIs should defer to the reporting requirements specific to their state.

Forming a Team and Communicating with Consumers

Many DOIs have divisions, such as consumer services sections, that work together to inform and protect insurance consumers. In the case of a disruptive cybersecurity event, providing the consumer services section with accurate, up-to-date information, scripts, and response templates will enable better consumer assistance. Such communication should be coordinated with and consistent with the messaging provided by the affected licensee prior to any consumer communication.

Therefore, DOIs should 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.

Communication with Law Enforcement and Other Regulators

During a cybersecurity event, law enforcement agencies and other regulators may request information from the responding DOI. Engaging with law enforcement officials and regulators can benefit overall

cybersecurity and inform the DOI's response, provided such communication is permitted under the relevant state regulation and necessary to prevent the spread of a cybersecurity event.

Overview of Lead State Concept

The Lead State concept has long been in use as part of financial surveillance and in market regulation. The following text from Section 1: Examination Overview – Determining the Lead State and Subgroups of Companies, from the *NAIC's Financial Condition Examiners' Handbook* explains the concept:

Every insurance holding company system has individual characteristics that make it unique. Therefore, an evaluation of traits is required to determine how examinations for the group should be coordinated and which individual state, known as the Lead State, should assume the leadership role in coordinating group examinations. The Lead State is charged with the coordination of all financial exams for the holding company group, as well as other regulatory solvency monitoring activities (*e.g.*, group supervision, including holding company analysis; group profile summary (GPS); assessments of the group's corporate governance and enterprise risk management (ERM) functions, etc.) as defined within the *NAIC's Financial Analysis Handbook*.

In most situations to date, the Lead State has emerged by mutual agreement (*i.e.*, self-initiative on its part and recognition by other states), generally as a result of the organizational structure of the group or as a result of the domicile of primary corporate and operational offices.

Additionally, the concept is also leveraged in the *NAIC's Market Regulation Handbook* within Chapter 4—Collaborative Actions – A Collaborative Action Guidelines says that:

In the case of Market Actions (D) Working Group actions, when selecting Lead States and Managing Lead States, the Market Actions (D) Working Group chair will consider at least the following criteria:

- The domestic regulator of the regulated entity;
- The top five premium volume and/or market share states;
- The referring states requested participation level;
- A state in which the identified issue appears to be more problematic;
- Geographic balance between zones;
- Specialized experience of a state's staff members;
- A state's experience in managing complex investigations or collaborative actions; and
- The ability to perform the duties and responsibilities of a Lead State and/or Managing Lead State.

While the Lead State concept varies in use related to cybersecurity events, it may be an appropriate means of creating efficiency while still allowing states to gather the information needed to support regulatory responses to cybersecurity events. As noted in the introduction, DOIs are encouraged to use the Lead State concept, where possible and appropriate.

Understanding and Receiving Notifications

As part of the information-gathering process, states should be mindful that only partial information may be available, and information provided may change as the licensee's investigation into the event proceeds.

Section 6 of Model #668 requires licensees to notify the insurance commissioner about cybersecurity events and to provide the DOI with as many of the following 13 pieces of information (from Section 6(B)) as possible:

- 1) The date of the cybersecurity event.
- 2) A description of how the information was exposed, lost, stolen, or breached, including the specific roles and responsibilities of third-party service providers, if any.
- 3) How the cybersecurity event was discovered.
- 4) Whether any lost, stolen, or breached information has been recovered and if so, how this was accomplished.
- 5) The identity of the source of the cybersecurity event.
- 6) Whether the licensee has filed a police report or has notified any regulatory, government, or law enforcement agencies and, if so, when such notification was provided.
- 7) A description of the specific types of information acquired without authorization. Specific types of information means particular data elements including, for example, types of medical information, types of financial information, or types of information allowing identification of the consumer.
- 8) The period during which the information system was compromised by the cybersecurity event.
- 9) The number of total consumers in this state affected by the cybersecurity event. The licensee shall provide the best estimate in the initial report to the commissioner and update this estimate with each subsequent report to the commissioner pursuant to this section.
- 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.
- 11) A description of efforts being undertaken to remediate the situation which permitted the cybersecurity event to occur.
- 12) A copy of the licensee's privacy policy and a statement outlining the steps the licensee will take to investigate and notify consumers affected by the cybersecurity event.
- 13) Name of a contact person who is both familiar with the cybersecurity event and authorized to act for the licensee.

The items listed above may require modifications for states adopting their own version of Model #668, or that have their own Cybersecurity related regulations. 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.

Receiving the above information will take some time, and some types of information may be available earlier than others. Notifications can be updated after a company reports the initial cybersecurity event; therefore, notification of an event should not be held up while all pertinent information is being compiled. The licensee who notified the DOI of a breach 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. Where possible, DOIs should establish clear and reasonable communication expectations with the licensee to ensure material updates provided are timely. If a cybersecurity event originated at a vendor, the DOI may wish to engage with the insurer to understand the impact the origin of the event will have on the notification and event response processes.

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.

Appendix A—Cybersecurity Event Notification Form {attached to this bulletin} provides an optional form that can be used to help states collect information.

Process for Responding to Cybersecurity Events

There may be at least three general points where a DOI can engage with a licensee after a cybersecurity event: 1) upon notification; 2) after the initial investigation; 3) or upon completion. A DOI's engagement with a licensee may vary based on the facts and circumstances of each cybersecurity event. Some questions to consider when making such a determination as to the appropriate scope of the DOI's engagement are as follows:

- What is known about the compromise, and is there an ongoing threat?
- Is there a greater threat to the insurance industry (*e.g.* through the involvement of third-party software many insurers use)?
- Has the licensee lost the ability to process transactions? Can they process claims? Can they process premiums?
- Can the licensee communicate with policyholders? Are their telephones, email, and website working?
- Has the licensee engaged in any general communication with policyholders? Is the licensee able to post a notice on its website? If so, when was the notice posted?
- Has law enforcement responded to the licensee's situation? What is their current level of involvement? Are they on-site?
- Are there other professionals on-site assisting with the recovery? What are their roles?

For a cybersecurity event that has been remediated and has a limited impact on daily operations and information technology (IT) operations, the DOI may let the licensee's investigation run its course before obtaining the necessary information.

If a DOI determines that further investigation is appropriate, then examining the licensee's response and remediation of the cybersecurity event to ensure policyholder data is secured may be warranted. There are several investigative options available to state insurance regulators, which are summarized in a document maintained by the NAIC's Cybersecurity (H) Working Group under the "Documents" tab on the Working Group's page – "[Summary of Cybersecurity Tools](#)." At a summary level, those tools include:

- Using the Powers of the Commissioner described in Model #668, if adopted and in effect.
- Investigating via the examination process described in the *NAIC's Financial Condition Examiners Handbook*.
- Investigating via the following checklists included in the *NAIC's Market Regulation Handbook*:
 - "Insurance Data Security Pre-Breach Checklist"
 - "Insurance Data Security Post-Breach Checklist"
- Ad-hoc inquiry, which may leverage the insights in the NAIC's [Cybersecurity Vulnerability Response Plan](#).

Note: the Cybersecurity (H) Working Group has a standing charge to provide educational forums/updates pertaining to these documents/materials.

In addition to these tools, a regulator is encouraged to coordinate oversight and reporting efforts with the federal agencies involved in an investigation. There is also potential value in coordinating with, or referencing referrals to the FBI Private Industry Notification (PIN) Network. Additional relevant information may also be obtained via the early 8-K filings under the SEC's Cyber Disclosure Rule. Some financial institutions may also be looking to the FTC's GLBA Safeguard Rule amendments addressing data breach notification.

Data Minimization

The principle of "data minimization, DOIs should consider when gathering information. Data Minimization means that a data controller should limit the collection of information to what is adequate (sufficient to properly fulfil your stated purpose), directly relevant (has a rational link to that purpose) and necessary to accomplish a specified purpose. The DOI should also retain the data only for as long as is necessary to fulfill that purpose. To do otherwise raise serious questions around data confidentiality and protection. DOIs should be particularly careful to limit collection of sensitive information such as vulnerable fields and configurations.

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.

When a licensee asserts that information required in MDL #668 is exempt due to attorney-client privilege or asserts that information requested by the state regulator is a trade secret or is otherwise confidential, a DOI should consult its legal counsel as how to proceed. A DOI may have to address concerns about confidentiality and the protection of their cybersecurity event information noting that Section 8(A) of MDL #668 provides confidentiality protections to the information submitted under Section 6(B). While every state has their own confidentiality and privacy regimes relating to cybersecurity event information, MDL #668 provides explicit confidentiality protection for most event information provided, as found in Section 8(A).

If a licensee is concerned about a specific document (*e.g.*, their forensics reports or other sensitive information) a DOI may consider performing a formal investigation described under Section 7(A) of MDL #668, which provides licensees with greater confidentiality. If a state's version of MDL #668 does not have comparable confidentiality protection, a limited-scope examination may offer similar confidentiality protection to the licensee. To the extent a DOI relies on third-party consultants for such investigations or examinations, DOIs may need to take steps to ensure that information viewed by the third-party consultants remains subject to the confidentiality provisions afforded under MDL #668.

CMA: Working Group to discuss - do we need to beef up the protections available under a ltd scope exam? Would that address some concerns about info being requested that can be reversed engineered? Able to address asking only for what is needed. But who defines 'needed'?

How to Receive Notifications and Acquire Required Information

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

Communication preferences within each DOI should generally be proactively communicated by DOIs with instructions on secured state webpages accessible only to licensees for how and where notifications should be submitted.

Additionally, DOIs may provide the licensee's outside counsel or third-party mitigation firm, if any, with a form requesting information. As noted above, information may be available at different times throughout the cybersecurity event lifecycle, and notifications can be updated after a licensee makes the initial report.

Appendix A: Sample Template (This is available in Excel format).

Information Provided		Company Response
Company Name		
1	Date of the cybersecurity event.	
2	Description of how the information was exposed, lost, stolen, or breached, including the specific roles and responsibilities of third-party service providers, if any.	
3	How the cybersecurity event was discovered.	
4	Whether any lost, stolen, or breached information has been recovered and if so, how this was done.	
5	The identity of the source of the cybersecurity event.	
6	Whether licensee has filed a police report or has notified any regulatory, government, or law enforcement agencies and, if so, when such notification was provided.	
7	Description of the specific types of information acquired without authorization. Specific types of information means particular data elements including, for example, types of medical information, types of financial information, or types of information allowing identification of the consumer.	
8	The period during which the information system was compromised by the cybersecurity event.	
9	The number of total consumers in this state affected by the cybersecurity event. The licensee shall provide the best estimate in the initial report to the commissioner and update this estimate with each subsequent report to the commissioner pursuant to this section.	
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.	
11	Description of efforts being undertaken to remediate the situation which permitted the cybersecurity event to occur.	
12	A copy of the licensee's privacy policy and a statement outlining the steps the licensee will take to investigate and notify consumers affected by the cybersecurity event.	
13	Name of a contact person and authorized to act for	



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

#

k

° # @

° = @

° h # @

V ° U @

CIS

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,

A handwritten signature in black ink that reads "Kirsten Wolfford". The signature is written in a cursive, slightly slanted style.

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 change 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 speak 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 investigating 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."

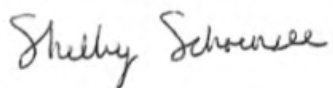
Conclusion

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

**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 1² 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.

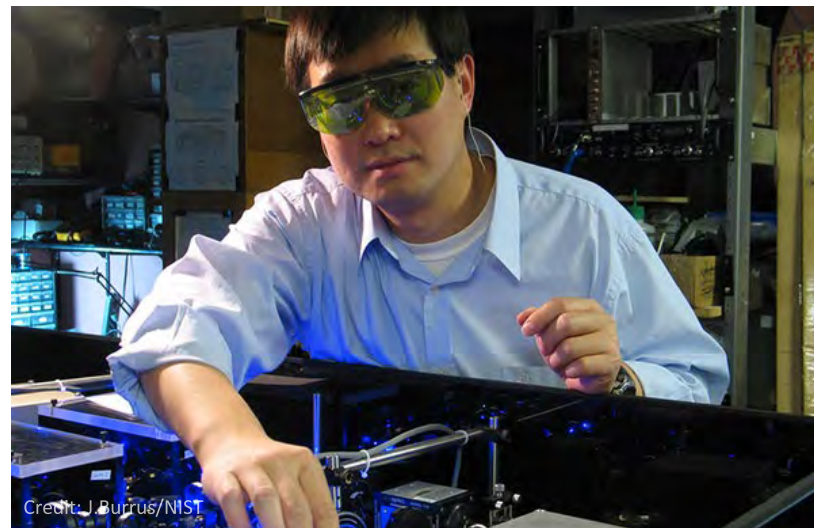
² NAMIC response (May 1, 2023) to NAIC Cybersecurity (H) Working Group Request for Input, Incident Response (March 26, 2023)

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**

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

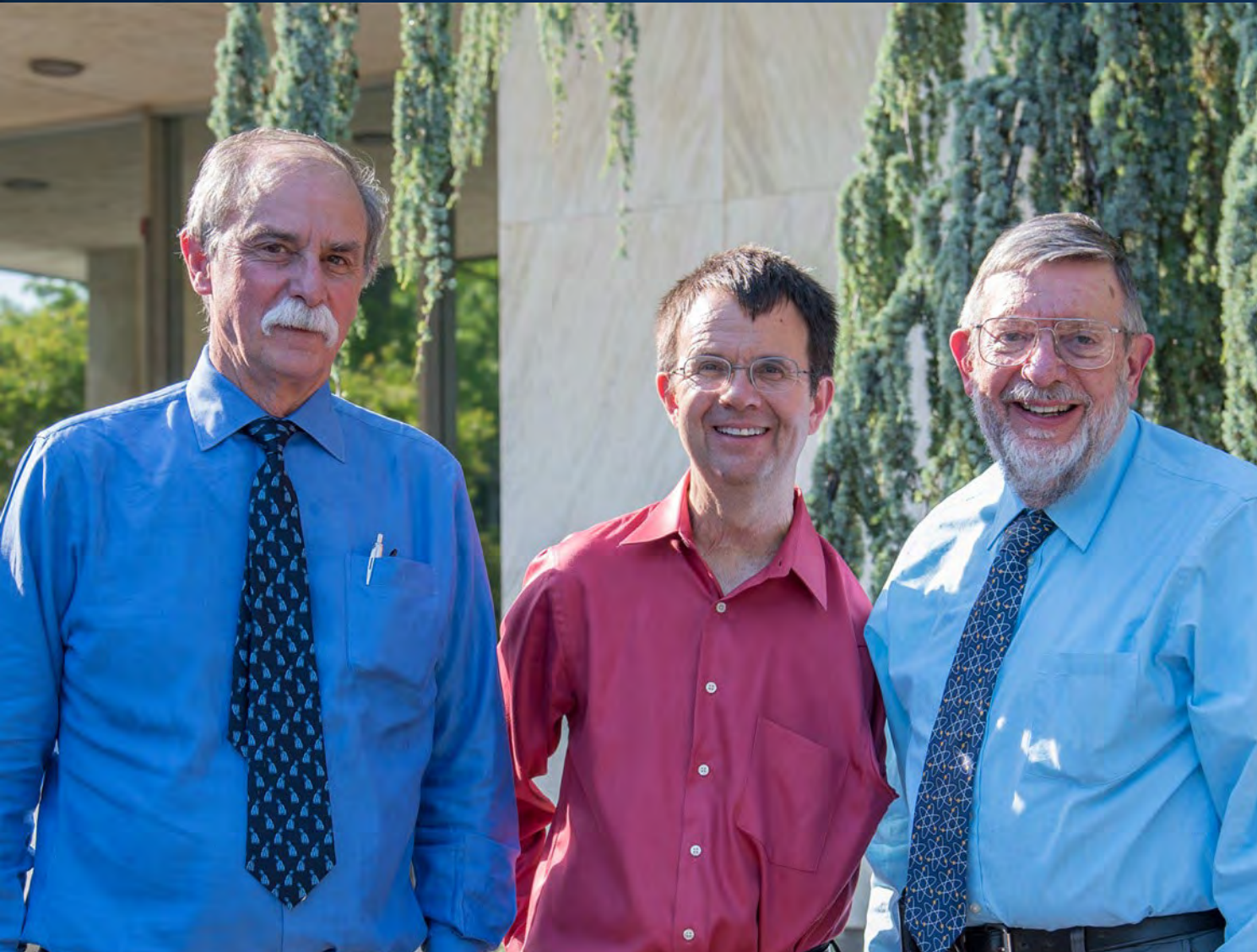


51
MANUFACTURING
EXTENSION
PARTNERSHIP CENTERS




U.S. BALDRIGE
PERFORMANCE
EXCELLENCE PROGRAM

NIST's Biggest Strength: Our Reputation




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

Critical & Emerging Technologies




ARTIFICIAL INTELLIGENCE
Transparent, trustworthy AI and machine learning



ADVANCED COMMUNICATIONS
(5G and beyond) and wireless technologies



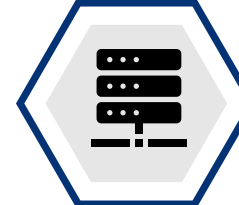
BIOTECHNOLOGY
And engineering biology to impact the health, agricultural, and industrial sectors



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



CYBERSECURITY AND PRIVACY
To enable the development and deployment of emerging technologies



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

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.

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:

- o concrete improvements to the Examples;
- o whether the Examples are written at an appropriate level of specificity and helpful for a diverse range of organizations;
- o what other types of Examples would be most beneficial to Framework users;
- o what existing sources of implementation guidance might be readily adopted as sources of Examples (such as the [NICE Framework Tasks](#));
- o how often Examples should be updated; and
- o 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 \(CPR T\)](#). 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.gov/document/discussion-draft-nist-cybersecurity-framework-20-core-implementation-examples



Discussion Draft

The NIST Cybersecurity Framework 2.0 Core with 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
		<p>applicable cybersecurity risks, and integrate them into organizational policies and applicable third-party agreements</p> <p>Ex7: Internally communicate cybersecurity supply chain risk management roles and responsibilities for third parties</p> <p>Ex8: Establish rules and protocols for information sharing and reporting processes between the organization and its suppliers</p>	
	<p>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)</p>	<p>Ex1: Identify areas of alignment and overlap with cybersecurity and enterprise risk management</p> <p>Ex2: Establish integrated control sets for cybersecurity risk management and cybersecurity supply chain risk management</p> <p>Ex3: Integrate cybersecurity supply chain risk management into improvement processes</p> <p>Ex4: Escalate material cybersecurity risks in supply chains to senior management, and address them at the enterprise risk management level</p>	
	<p>GV.SC-04: Suppliers are known and prioritized by criticality</p>	<p>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</p> <p>Ex2: Keep a record of all suppliers, and prioritize suppliers based on the criticality criteria</p>	
	<p>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)</p>	<p>Ex1: Establish security requirements for suppliers, products, and services commensurate with their criticality level and potential impact if compromised</p> <p>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</p> <p>Ex3: Define the rules and protocols for information sharing between the organization and its suppliers and sub-tier suppliers in contracts</p> <p>Ex4: Manage risk by including security requirements in contracts based on their criticality and potential impact if compromised</p>	

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)

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

- **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.**

STAY IN TOUCH

CONTACT US



NIST.gov



@NISTcyber

Receive an Update on Federal Activities Related to Cybersecurity

Discuss Any Other Matters