November 14, 2022

Submitted via the Federal eRulemaking Portal: http://www.regulations.gov

The Honorable Janet Yellen
Secretary
U.S. Department of the Treasury
1500 Pennsylvania Avenue NW
Washington, DC 20220

RE: Potential Federal Insurance Response to Catastrophic Cyber Incidents [87 FR 59161]

Dear Secretary Yellen,

The College of Healthcare Information Management Executives (CHIME) and the Association for Executives in Healthcare Information Security (AEHIS) respectfully submit our comments to the U.S. Department of the Treasury in response to the "Request for Comment" regarding the *Potential Federal Insurance Response to Catastrophic Cyber Incidents*, as published in the *Federal Register* on September 29, 2022 (Vol. 87, No. 188).

Background

CHIME is an executive organization dedicated to serving chief information officers (CIOs) and other senior healthcare IT leaders in hospitals, health systems and other healthcare settings across the country. Consisting of more than 2,900 members in 60 countries, our members are responsible for the selection and implementation of clinical and business technology systems that are facilitating healthcare transformation. Launched by CHIME in 2014, AEHIS represents more than 950 healthcare security leaders and provides education and networking for senior IT security leaders in healthcare. CHIME and AEHIS members are among the nation's foremost health IT experts, including on the topics of cybersecurity, privacy and the security of patient and provider data and devices connecting to their networks.

Key Recommendations

In our comments, we provide responses to address the specific questions included in the Request for Comment regarding a *Potential Federal Insurance Response to Catastrophic Cyber Incidents*.[1] First, we thank the U.S. Department of Treasury (Treasury) and the Federal Insurance Office (FIO) within Treasury for their ongoing efforts regarding both cyber insurance and insurer cybersecurity. CHIME applauds the Treasury's FIO for undertaking the joint assessment with the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA), as recommended by the Government Accountability Office (GAO)[2], to determine "the extent to which risks to critical infrastructure from catastrophic cyber incidents and potential financial exposures warrant a federal insurance response." CHIME and AEHIS are pleased to offer our comments to inform the FIO's future work and the joint assessment on the Request for Comment's questions related to cyber insurance and catastrophic cyber

[1] United States, Department of the Treasury. Potential Federal Insurance Response to Catastrophic Cyber Incidents. Vol. 87 Fed. Reg. 59161. Published September 29, 2022. https://www.federalregister.gov/documents/2022/09/29/2022-21133/potential-federal-insurance-response-tocatastrophic-cyber-incidents

[2] *Cyber Insurance: Action Needed to Assess Potential Federal Response to Catastrophic Attacks*. (2022, June 21). U.S. GAO. Retrieved October 25, 2022, from https://www.gao.gov/products/gao-22-104256

incidents. Recent incidents – including attacks targeting healthcare and other essential services during the COVID-19 pandemic – illustrate the importance of preparing for future cyberattacks and their financial toll.[2] **As part of advocacy efforts surrounding cybersecurity, we polled our membership in a survey[1] to better understand the threats our members face, the resources they need and the education gaps that currently exist. The results continue to outline what those who have been active in the cybersecurity landscape have known for years, healthcare is under constant threat, more resources are needed for healthcare providers and significant education gaps remain.**

Per the Request, our responses also include: (1 the data or rationale, including examples, supporting any opinions or conclusions; and (2 any specific legislative, administrative, or regulatory proposals for carrying out recommended approaches or options. **CHIME strongly supports policies that:**

1) incent good cyber hygiene including federal policies that provide financial and other forms of assistance;
2) result in shared responsibility;
3) foster information sharing;
4) reduce punitive approaches that treat victims of attacks as criminals;
5) encourage use of the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)[23]; and
6) create incentive-driven approaches to improving the cybersecurity posture of providers.

CHIME and AEHIS members believe a federal insurance response is warranted – for the reasons discussed in our comments – and hopes that our input will assist in informing the FIO as they consider a potential federal insurance response to catastrophic cyber incidents in critical infrastructure sectors. Furthermore, we agree with the GAO that any federal insurance response should include clear criteria for coverage and specific cybersecurity requirements.

Detailed Recommendations

Cyber threats to critical infrastructure represent a significant risk to the nation's economic stability. Critical infrastructure refers to the systems and assets, whether physical or virtual, so vital to the United States that their incapacity or destruction would have a debilitating effect on security, national economic security, economic stability, national public health or safety, or any combination of those matters.[5] Over the past several years, the FIO has continued its ongoing efforts with regard to both cyber insurance and insurer cybersecurity. As Treasury acknowledges, cyber insurance is a significant risk-transfer mechanism, and the insurance industry has an important role to play in strengthening cyber hygiene and building resiliency.

According to the GAO, the Department of the Treasury's FIO and the DHS's CISA both have taken steps to understand the financial implications of growing cybersecurity risks. However, they have not assessed the extent to which risks to critical infrastructure from catastrophic cyber incidents and potential financial exposures warrant a federal insurance response. Because CISA is the primary risk advisor on critical infrastructure and FIO the federal monitor of the insurance sector, the GAO found that they are wellpositioned to jointly perform such an assessment.[2]

Catastrophic Cyber Incidents

"Healthcare and Public Health (HPH) sector organizations have been the targets for malicious cyber activity for the past 10 years. Most recently, COVID-19 has highlighted the need for HHS to pay continuous attention

[1] *Survey of Members*. The College of Healthcare Information Management Executives (CHIME) and The Association for Executives in Healthcare Information Security **(**AEHIS). August 2021. https://chimecentral.org/wpcontent/uploads/2021/08/PP_infographic-v5_Handout.pdf
[2] *Updating the Cybersecurity Framework – Journey To CSF 2.0*. (2022, September 21). NIST. Retrieved October 25, 2022 from https://www.nist.gov/cyberframework/updating-nist-cybersecurity-framework-journey-csf-20
[3] U.S.C. § 5195c(e). See Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act).

to cyber threats, which pose a serious challenge to national security, economic well-being, and public health and safety."[4] Recent incidents – including attacks targeting health care and other essential services during the COVID-19 pandemic – illustrate the importance of preparing for future cyberattacks and their financial toll.[2] According to our survey, 67 percent of respondents indicated that they'd had a security incident during August 2020 to August 2021. On average, individual data breaches cost healthcare organizations in excess of $10 million – including costs related to detection, response, and loss of business – an increase of 41.6 percent since 2020, according to IBM's annual Cost of Breach Report released in July 2022.[5] Healthcare data security breaches in particular have the potential to cost even more when fines, litigation, and damaged reputation are considered.

Cyberattacks pose a persistent threat to patient safety and our national security. As one of our members stated in testimony to the National Committee on Vital and Health Statistics (NCVHS) Subcommittee on Privacy, Confidentiality and Security last year, "Cybersecurity incidents are not only a threat to national security, they are also a threat to patient safety, as attacks can cause denial of service, medical device corruption, and data manipulation that directly impacts clinical operations, patient care and public health. In addition, healthcare data and information remain lucrative targets for theft and exploitation, particularly through ransomware attacks and COVID themed social engineering by criminal groups and adversarial nation states."[8] The techniques used are the same ones that have been successfully used against large, publicly traded companies with far greater resources than most healthcare providers.

Potential Federal Insurance Response for Catastrophic Cyber Incidents

Some insurance companies offer businesses cybersecurity coverage, or cyber insurance, to share the risk of losses from an event that jeopardizes the confidentiality, integrity, and availability of an information system. The insurance can be provided through a stand-alone policy with only cyber coverage or as a part of a packaged policy with multiple types of coverage. Cyber insurance coverage is available for both first-party (policyholder) and third-party liability losses (policyholder's clients or customers). According to data from The National Association of Insurance Commissioners (NAIC), cyber insurance coverage represents less than 1 percent of the premiums written in the property and casualty insurance market.[2]

Cyber insurance provides coverage for common cyber risks to help companies mitigate losses related to cyber incidents and can encourage policyholders to manage cyber risk. But cyber insurers have been limiting their exposure to systemic losses (including by limiting coverage), and cyber carriers may not fully cover losses from a systemic event with catastrophic losses. Moreover, while cyber incidents could be covered under the Terrorism Risk Insurance Program (TRIP), certifying these incidents as acts of terrorism could be challenging.[2] Acts of war, including cyber war, can have cascading consequences across entire systems.[67] Contractual definitions of "act of war" vary – and "act of war" exclusions are generally found in policies issued in most lines of insurance, including cyber.[2] However, insurers and TRIP will not cover damages caused by cyberattacks in some cases; for example, they may only cover cyberattacks if they can be considered "terrorism" under its defined[10] criteria.

Many insurers also have increased premium rates in response to increasing losses. Various sources show considerable increases in cyber insurance premium rates in the past year. According to the NAIC's *Cyber*

---

[4] *Cybersecurity: HHS Defined Roles and Responsibilities, but Can Further Improve Collaboration*. (n.d.). U.S. GAO. Retrieved October 25, 2022, from https://www.gao.gov/products/gao-21-403

[5] *Cost of a data breach 2022*. (n.d.). IBM. Retrieved October 25, 2022, from https://www.ibm.com/reports/data-breach

[8] *The National Committee on Vital and Health Statistics (NCVHS) Subcommittee on Privacy, Confidentiality and Security Hearing*. (July 21, 2021). National Committee on Vital and Health Statistics. Retrieved October 25, 2022, from https://ncvhs.hhs.gov/meetings/subcommittee-on-privacy-confidentiality-and-security-3/.*Testimony of Erik Decker*. Retrieved October 25, 2022, from https://chimecentral.org/wp-content/uploads/2021/07/1A-Decker-WrittenTestimony-only.pdf

[6] Bateman, J. (2020, October 5). *War, Terrorism, and Catastrophe in Cyber Insurance: Understanding and Reforming Exclusions*. Carnegie Endowment for International Peace. Retrieved October 25, 2022, from https://carnegieendowment.org/2020/10/05/war-terrorism-and-catastrophe-in-cyber-insurance-understanding-andreforming-exclusions-pub-82819

[7] U.S.C. § 2331(4)

Insurance report[8], the 2021 data shows a cybersecurity insurance market of roughly $6.5 billion, reflecting an increase of 61 percent from the prior year. The Council of Insurance Agents & Brokers reported a more than 34 percent increase in cyber premium rates from the third to the fourth quarter of 2021.[12] The Council of Insurance Agents & Brokers survey notes that respondents pointed to an increased frequency and severity of cyber claims, as well as the difficulty of quantifying cyber risk, as a reason for the significant increases.

Over 80 percent of the respondents in CHIME and AEHIS's survey indicated that the cost of cyber insurance had increased over the past year. Thirty-three percent of respondents reported an increase of as much as 25 percent; 21 percent reported an increase of as much as 50 percent; and 10 percent reported an increase of as much as 100 percent. Notably, 16 percent of respondents reported an increase in the cost of cyber insurance of more than 100 percent.

Starting in 2020, cyber insurance began moving towards a hard market – with insurers responding, in part, by increasing premiums; this trend has continued throughout 2021 and into 2022.[9] A hard market is defined as "an insurance market cycle where insurers reduce the amount of coverage they are willing to write, causing supply to contract and premiums to rise."[9] The direct written premiums in the admitted market rose by 74 percent in 2021. Insurers saw a reduction in their loss ratios, in part because of premium increases. Additionally, "companies continued to see their premiums increase during the first quarter of 2022."[9] Private insurers are continuing to limit their potential losses from systemic cyber events by excluding coverage for losses from cyber warfare and infrastructure outages.

According to CHIME and AEHIS members, based on the annual renewal process they are currently going through – their premiums are continuing to increase, and the average annual increases in premiums that they are experiencing **each year have typically doubled**, if not more. One member noted that they were paying a $1 million dollar premium for each $5 million dollars of coverage. Some members have reported being denied any cyber insurance coverage – simply because they had experienced a cyberattack within the last five years and are therefore required to "self-insure." Furthermore, even when our members have "comprehensive" cyber insurance, the coverage may only cover half of their losses – often amounting to tens of millions of dollars that they are then left to recoup.

Hospitals and healthcare delivery organizations (HDOs) are extraordinarily complex organizations with many typical organizational characteristics dialed up to extremes – such as a technology saturated environment and complex internal politics. While they are similar to other organizations as far as operating in a technology saturated environment, they must manage an array of devices ranging from legacy information technology (IT) to connected medical devices. And, unlike other organizations, the sheer scale and magnitude of devices is nearly immeasurable – some are procured not by a single IT department but purchased ad hoc by clinicians, purchased from medical device companies, and others brought in by patients. While HDOs deal with the same internal politics that other large organizations do, it is further complicated by the complexity of the functions in the healthcare sector – they are not just dealing with the traditional finance and IT departments. They must also support departments that include radiology, oncology, cardiology, and pediatrics, to name a few. The degree of specialization within each department is high, requiring completely different equipment, addressing differing patient needs, differing workflows, and employing a highly specialized labor force that requires years of training.[10]

Like nearly all organizations in the United States, hospitals and HDOs must care – to some degree – about their ability to generate positive net revenue in order to keep their doors open. However, they are unlike other organizations in that their first and most important mission is to care for their patients. The increasing

[8] *NAIC Report Shows Premiums Grew 61% as Cyberthreats Rose in 2021*. (October 21, 2022). NAIC. Retrieved October 25, 2022, from https://content.naic.org/article/naic-report-shows-premiums-grew-61-cyberthreats-rose-2021
[12] The Council of Insurance Agents & Brokers. (2022, August 15). *P/C Market Surveys – Commercial Property/Casualty Market Index: Q4/2021*. Retrieved October 25, 2022 from https://www.ciab.com/market-intel/pcmarket-index-survey/
[9] Staff, T. (2012, October 19). *HARD MARKET*. The Law Dictionary. Retrieved October 25, 2022 from https://thelawdictionary.org/hard-market/
[10] Jalali, M. S., & Kaiser, J. P. (2018). Cybersecurity in Hospitals: A Systematic, Organizational Perspective. *Journal of medical Internet research*, *20*(5), e10059. Retrieved October 25, 2022, from https://doi.org/10.2196/10059

cost of cyber insurance is becoming untenable for healthcare providers, and at times – unattainable. Hospitals and healthcare systems are not only critical to their communities in that they provide care to them, they are often the largest employers.

Between 2009 and 2021, 4,419 healthcare data breaches of 500 or more records have been reported to the Department of Health and Human Services' (HHS) Office for Civil Rights (OCR) as required under the Health Insurance Portability and Accountability Act (HIPAA). Those breaches have resulted in the loss, theft, exposure, or impermissible disclosure of 314,063,186 healthcare records – equating to nearly 95 percent of the 2021 population of the United States. In 2021, an average of 1.95 healthcare data breaches of 500 or more records were reported each day, double the number of reported breaches only four years prior.[11] **When hackers and/or bad actors gain access to patient records and information, they will have the ability to change and manipulate patient data – which could have disastrous consequences to each individual patient. Two out of three of respondents to CHIME and AEHIS's cybersecurity survey reported having had a security incident occur in the past 12 months.**

Our members are committed to cybersecurity best practices and take their responsibility to protect not only the privacy and security of patient data and devices networked to their system – but critically – their patient's overall safety and well-being very seriously. Currently, hospitals are forced to balance the high cost of cyber insurance, inherent risks to their patients, and the current workforce shortage needed to mitigate these risks. Globally, the shortage of cybersecurity professionals is estimated to be 2.72 million.[12] A recent study suggests that the global cybersecurity workforce needs to grow 65 percent to effectively defend organizations' critical assets.[13] The ISACA State of Cybersecurity Survey[14] responses confirm this struggle, with 60 percent of respondent enterprises experiencing difficulties retaining qualified cybersecurity professionals in 2021, which is a seven-percentage-point increase from 2020 (53 percent). Healthcare provider organizations face further barriers as security staff are often lured away to other more lucrative sectors with the ability to pay higher salaries, thus not only is there is recruitment an issue but also retention.

Hospitals and HDOs often face difficulty allocating resources to secure their environments. This will be an ongoing challenge for years to come, particularly related to the rapidly growing Internet of Things (IoT) and Internet of Medical Things (IoMT) sphere. A recent survey from Cynerio and the Ponemon Institute found that the typical information technology (IT) spend for respondents averages $145 million in the fiscal year and an average of 17 percent of that spend is focused on IT security. Of that security spend, an average of 20 percent was reported to go towards IoT/IoMT device security – an average of $5 million in the fiscal year.[15]

The Food and Drug Administration (FDA) acknowledged in recent draft guidance that "in the context of cybersecurity, security risk management processes are critical because, given the evolving nature of cybersecurity threats and risks, no device is, or can be, completely secure. Security risk management should be part of a manufacturer's quality system."[16] The FDA further stated that because of the lack of " adequate cybersecurity considerations across all aspects of these systems, a cybersecurity threat can compromise the safety and/or effectiveness of a device by compromising the functionality of any asset in the system. As a result, ensuring device safety and effectiveness includes adequate device cybersecurity, as well as its security as part of the larger system."

---

[11] *Healthcare Data Breach Statistics - Latest Data for 2022*. (2022, August 26). HIPAA Journal. Retrieved October 25, 2022, from https://www.hipaajournal.com/healthcare-data-breach-statistics/

[12] National Institute of Standards and Technology (NIST). (2022, September 29). *Cybersecurity Workforce Demand*. NIST National Initiative for Cybersecurity Education (NICE). Retrieved October 25, 2022, from https://www.nist.gov/system/files/documents/2022/07/06/NICE%20FactSheet_Workforce%20Demand_Final_20211202.pdf

[13] *A Resilient Cybersecurity Profession Charts the Path Forward: (ISC)² Cybersecurity Workforce Study, 2021*. (2021). www.isc2.org. Retrieved October 25, 2022, from https://www.isc2.org//-/media/ISC2/Research/2021/ISC2Cybersecurity-Workforce-Study-2021.ashx

[14] *State of Cybersecurity 2022*. (2022, April 23). ISACA. Retrieved October 25, 2022, from https://www.isaca.org/state-of-cybersecurity-2022

[15] Cynerio & Ponemon Institute. (2022). *The Insecurity of Connected Devices in Healthcare 2022*. Retrieved October 25, 2022, from https://www.cynerio.com/blog/cynerio-and-ponemon-study-finds-frequent-cyber-attacks-andinsufficient-accountability-in-healthcare-notably-impact-patient-care

[16] Center for Devices and Radiological Health (CDRH). (2022, April 8). *Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions*. U.S. Food And Drug Administration. Retrieved

HDOs are not provided with, nor can they expect, for example, a medical device company to estimate the total costs of a cybersecurity attack related to a device – despite the fact that any cybersecurity vulnerability may cost them millions of dollars. Yet, they are still bearing the entire burden of ensuring the cybersecurity of every device – including those that are brought into their organization by patients, and the scope is not limited to devices that are network-enabled or contain other connected capabilities. **Our survey found that nearly 60 percent of members reported that the IoT and connected devices were their largest area of concern for risk of cyber intrusion over the next three years.** Healthcare provider organizations continue to face challenges when they purchase medical devices that arrive with vulnerabilities, as well as, protecting devices that are no longer being supported by manufacturers or contain software that is obsolete. The cost to replace these devices simply exceeds healthcare systems' and providers' budgets.

The NAIC states that: "Because of the increasing cybersecurity risks, businesses are facing a more demanding underwriting process. Insurers are more thoroughly examining a company's security controls, internal processes, and procedures concerning cyber risk. Additionally, underwriters are more cautious in examining an insured's risk presented by the third parties working or contracting with the insured."[9] HDOs do not have a choice to simply "not work with" or "not contract with" third party vendors – yet they are being penalized or deemed uninsurable despite the fact that there is not a streamlined process to ensure HDOs are aware of any new potential and/or known vulnerabilities with medical devices. While every HDO must determine their own risk – CHIME and AEHIS have urged the FDA to require device manufacturers to: 1) clearly elucidate the potential risks and failures if someone continues to use the device "as is"; and 2) clearly communicate the potential risks and failures that any "interim mitigation process" may create and/or introduce, including to the patient and any ecosystem the medical device may be connected to. Furthermore, even if there is not a "patch" or "update" yet available for a known vulnerability or critical update – medical device manufacturers are not required to alert providers in a *timely* manner, which is essential to patient safety, as well as building and maintaining a strong, robust medical device safety net. The FDA is seeking greater authority to regulated medical devices from congress, something we strongly support.

Whether they are in a patient's room or the hospital laboratory, both medical devices and other devices – such as a patient's mobile device – rely on network connectivity for operations and maintenance. Additionally, nearly all of the technology components in these devices are not developed by the HDO. These components include software, services, and hardware development from organizations known as third parties. One study found that the average number of third parties that organizations contracted with in 2021 was 1,950 and anticipated an increase to an average of 2,541 in 2022. Further, it notes that: "Third-party products and services are a necessary and critical part of the HDO IT blueprint, but each brings another set of risk factors to the table. Some risks are inherent to the third party such as secure operating systems and other software in medical devices […] the risk created by the third party or the HDO use of the third party needs to be managed. **The burden is on the HDO to perform assessments throughout their relationship with the third party (e.g., procurement, implementation, usage, updates, termination, etc.)."**[17]

In structuring a potential federal insurance to catastrophic cyber incidents, CHIME and AEHIS urge the FIO to take into consideration that all devices be considered part of the entire ecosystem when they enter the four walls of a hospital. For example, one underwriting questionnaire set included questions regarding the "loss of tech support" – in other words, does the organization use any software or hardware that is no longer supported or has been identified as end-of-support by the software or hardware vendor. When patients bring their own devices into a hospital or HDO, or a medical device manufacturer fails to convey all the vulnerabilities to healthcare CIOs and CISOs, it severely limits end-users – ultimately the clinicians – and the critical capability to ensure that the devices are secure. Furthermore, the post market mitigation process when cybersecurity threats arise is already complex for end-users. While providers may not be able to completely avoid every cybersecurity incident, steps taken to decrease the timeline between the discovery of the threat and mitigation of the threat is essential to increasing patient safety. **Cybersecurity risks are already inherently transferred to healthcare providers and patients as soon as the device enters the supply chain. Thus, the risk analysis of any device should not be solely incumbent upon the provider – it must be a shared responsibility.**

[17] Ponemon Institute & Sponsored by Censinet. (2021). *The Impact of Ransomware on Healthcare During COVID-19 and Beyond*. https://www.censinet.com/wp-content/uploads/2021/09/Ponemon-Research-Report-The-Impact-ofRansomware-on-Healthcare-During-COVID-19-and-Beyond-sept2021-1.pdf

A recent study found that about half (45 percent) of cyberattacks resulted in adverse impact on patients. About half (53 percent) of those with adverse impacts on patient care report increased mortality rates after a cyberattack (24 percent overall). About half (56 percent) have experienced one or more cyberattacks in the last 24 months. Almost half (43 percent) have experienced at least one ransomware attack in the last 24 months. When cyberattacks result in adverse patient care, patients face risks including high rates of impacted service (54 percent) and inappropriate therapy or treatment deliveries (26 percent). Furthermore, "for every reported set of vulnerabilities related to hospital robots or infusion pumps, there are likely thousands more that are unknown and far more dangerous."[6]

Hospitals and HDOs need and want help in obtaining and being able to afford cyber insurance – and they would be eager accept assistance. CHIME and AEHIS's survey found that 40 percent of our members would be interested in grants and/or federal assistance and 17 percent would like closer relationships with federal authorities (i.e., the Federal Bureau of Investigations (FBI) and CISA). As health services make use of a variety of medical devices, interconnectivity and interoperability create issues as they are now being accessed from outside health services' internal network perimeter.[18] **Our members are committed to utilizing and having in place all the resources and process at their disposal – even when resources are scarce – to manage, monitor, and mitigate cybersecurity risks to the best of their ability. They are dedicated to best practices regarding cyber hygiene, as well as the daunting tasks involved with the monitoring of risk across third parties. They undertake all of these efforts because they are truly committed to the safety of their patients. It should be noted, however, that the ability of all healthcare providers to make needed investments in cyber is extremely limited for safety-net providers and other small and under-resourced entities.**

Members of CHIME and AEHIS use a variety of security authentication measures to manage authorized users – including, but not limited to – knowledge-based authentication measures (i.e., passwords); possession-based authentication measures; location-based authentication measures; inherence-based authentication measures (i.e., biometrics); and behavior-based authentication measures. They regularly conduct cybersecurity activities including, but not limited to, wireless penetration testing; risk (i.e., identify compliance gaps and security vulnerabilities); cybersecurity maturity; tabletop exercises or drills; third parties/vendors; vulnerability scanning; red/blue team exercises; IT/security; system/application audits; and enterprise. Many members of CHIME and AEHIS participate in a variety of information sharing and analysis organizations – including the Health Cybersecurity & Communication Integration Center (HC3) and the Health Information Sharing and Analysis Center (H-ISAC) – to identify cybersecurity threats and vulnerabilities. Due to this participation, the information provided by our members is incredibly valuable to CISA, because they are able to get a broad section of the healthcare sector reporting – and can evaluate emerging trends. Over 90 percent of our members participate with DHS CISA in order to identify cybersecurity threats and vulnerabilities. Over 80 percent of CHIME and AEHIS members surveyed include an inventory of all business vendors and an evaluation of all high-risk vendors as part of their third-party risk management program. Nearly 70 percent of our members surveyed rank business vendors based on the potential risk they post to their organization.

The Request specifically asks the following questions: 1) What data do you collect that you would be willing to share with FIO and/or CISA to consider in their assessment of catastrophic cyber incidents and cyber insurance?; 2) What other information regarding catastrophic cyber incidents and cyber insurance should FIO and CISA consider?; and 3) What data should FIO and/or CISA consider collecting to help inform this assessment and their ongoing work? CHIME and AEHIS would welcome the opportunity to provide additional information that may be helpful in ongoing efforts related to a Potential Federal Insurance Response to Catastrophic Cyber Incidents. As noted earlier, our members are executives and senior healthcare IT and security leaders – and we are offering to continue to serve as a resource to FIO and/or CISA. Working together through the rulemaking process is just one way we can accomplish our shared goals and make meaningful changes in healthcare. Our members are extremely knowledgeable and have decades of experience executing cyber hygiene best practices and lessons learned in their own healthcare systems and delivery organizations. We look forward to continuing to be a trusted stakeholder and resource to FIO and CISA.

[18] He Y, Aliyu A, Evans M, Luo C. *Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review*. J Med Internet Res 2021;23(4):e21747. Retrieved October 25, 2022, from https://www.jmir.org/2021/4/e21747

Conclusion

We appreciate the opportunity to provide comments and help inform the important work being done by Treasury's FIO and CISA. CHIME and AEHIS appreciate the issuance of this important Request for Comment regarding a Potential Federal Insurance Response to Catastrophic Cyber Incidents. As Treasury notes, cyber incidents impacting critical infrastructure have increased in frequency and severity. Cyber insurers are increasingly limiting their exposure to losses by limiting coverage, and the cyber insurance market often does not cover losses from a systemic event with catastrophic losses.

Our members believe, based on experience, that the current marketplace for cyber insurance offered to the healthcare sector is tenuous, financially unfeasible, and for some – completely unavailable. Therefore, we are supportive and appreciative of the Treasury's consideration to implement a federal insurance response to catastrophic cyber incidents. Creating this opportunity for stakeholders to engage – especially members of critical infrastructure sectors is an essential part of policymaking. CHIME members prioritize their patients and the communities they serve. We look forward to supporting the Treasury in its efforts to implement a new federal insurance response to assist hospitals and HDOs, and ultimately – protect patients. CHIME has long stood as staunch supporters of all efforts in both Congress and the federal agencies that ensure patient data stays secure and is never compromised in a way that could jeopardize patient care or trust in the American healthcare system. We will continue to support new and continued efforts to build on these important policies and welcome Treasury action.

In closing, we would like to thank the Treasury Department for providing the opportunity to comment on this important Request for Information. Should you have any questions or if we can be of assistance, please contact Chelsea Arnone, Director, Federal Affairs at carnone@chimecentral.org.

Sincerely,

Russell P. Branzell, CHCIO, LCHIME
President and CEO
CHIME