March 22, 2019

The Honorable Mark Warner
U.S. Senate
703 Hart Senate Office Building
Washington, DC 20510

Re: Healthcare Cybersecurity Request for Information

Dear Senator Warner,

The College of Healthcare Information Management Executives (CHIME) and the Association for Executives in Healthcare Information Security (AEHIS) are pleased to respond to your request for information concerning the state of healthcare cybersecurity. As senior health information technology and security leaders, we welcome the opportunity to share our perspectives on how we can better secure our health system.

CHIME is an executive organization dedicated to serving chief information officers (CIOs) and other senior healthcare IT leaders. Consisting of more than 2,800 members in 51 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 850 chief information security officers (CISOs) 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 topic of cybersecurity and they take their responsibility to protect the privacy and security of patient data and devices networked to their system very seriously.

Healthcare is deemed a critical infrastructure by the Department of Homeland Security (DHS) and as such, patient safety and patient data should be viewed as a public good; protecting those things should be a national priority. We applaud your willingness to address the state of healthcare cybersecurity. Cybersecurity attacks are highly disruptive and can be crippling to healthcare entities, as illustrated by the WannaCry and Petya ransomware attacks in 2017. Providers with limited resources struggle to balance the huge demands for cybersecurity technology and information risk management programs. Threats to healthcare organizations are growing more sophisticated every day and too many health systems are not properly equipped to combat the myriad of attacks that could penetrate their networks. Healthcare entities grapple daily with an onslaught of cybersecurity threats, both to patient data and the systems in use to provide life-saving care. While the cybersecurity posture of the sector has improved, there remains a great way to go.

In 2017 CHIME partnered with KLAS Research on a healthcare industry cybersecurity benchmarking report. The following findings provide an outline of the current state of cybersecurity within healthcare organizations:

- Nearly all organizations have someone in charge of their security program, though that role is sometimes filled by someone who is not solely dedicated to IT security.

- 40% of organizations have a VP/C-level in charge of their program. About half of these are CISOs; the other half are CIOs/Chief Technology Officers (CTOs).
- Compared to those in an IT role, respondents with a security background more often report having a vice president or director (often a CISO or security director) in charge of their security program. They are also significantly more likely to have a cybersecurity framework in place and a deeper breach-readiness level.
- Only 16% of organizations feel they have a fully functional security program; nearly all of these are integrated delivery networks (IDNs) or larger hospitals.
- More than half of organizations still developing their security program are spending less than 3% of their total IT budget on security. As they begin to build out more robust programs, organizations are more likely to spend a higher percentage of their budget on security, likely due to increased staff, infrastructure, and software costs.
- By far, the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)is the most commonly used framework.[1]

We appreciate the opportunity to share our answers to your provided questions below.

1. **What proactive steps has your organization taken to identify and reduce its cyber security vulnerabilities?**

CHIME and AEHIS members take their responsibility to secure and protect patient data and the lifesaving systems that health systems rely on very seriously. Health systems have increased investments in wide-scale efforts to reduce their attack surfaces. Health systems are reducing the number of vendors being used and growing security teams but doing so with limited financial resources. While efforts are underway to improve the cybersecurity hygiene of the industry, accord to the 2018 CHIME HealthCare's Most Wired Survey, only 29 percent of the 618 health systems had a comprehensive security program in place.

Our members often design their multi-tiered security programs to follow the NIST CSF to identify and reduce cyber security vulnerabilities. This was echoed in the 2018 CHIME HealthCare's Most Wired Survey with 78 percent of the more than 600 respondents reporting they adopted the NIST CSF. Some of the technologies in use by health systems for adherence to the NIST CSF include, but are not limited to:

- Vulnerability Management – The cyclical practice of identifying, classifying, remediating and mitigating vulnerabilities, typically through automated technology. This includes both tactical and strategic remediation (such as patching) and/or deploying risk reducing mitigations. This may include multiple active vulnerability scanning solutions as well as automated remediation technology.
- Network Segmentation – Logically isolating or reducing exposure of critical systems in order to reduce exposure to an attack surface/
- Intrusion Prevention – Network and host-based technology that can actively and automatically prevent an intrusion from occurring.
- Data Loss Prevention – Policy, processes and technology that prevents sensitive information (such as protected health information) from leaving organizational designated security boundaries.
- Traffic Filtering – Web, email, network control traffic or other techniques that identify and prevent access to potentially malicious content.

Healthcare organizations are largely adopting a risk-based approach to cybersecurity and risk mitigation. Healthcare CIOs and CISOs are following guidance from NIST, including 800-30 for risk assessment. Unfortunately, to date, much of the risk assessment efforts have been limited to those risks posed by electronic health records (EHRs) and not across the entire enterprise. As technology has proliferated in healthcare, it is imperative that risk is characterized accordingly.

[1] "Cybersecurity 2017, Healthcare Provider Security Assessment." A KLAS-CHIME Benchmarking Report"

While some members point to their participation in information sharing organizations, formal participation is quite limited across health systems. The 2018 Most Wired Survey found that while most organizations participate informally—by sharing information within a professional society or health IT user groups—less than one-third participate with formal groups such as the Health Information Sharing and Analysis Center (H-ISAC), Cyber Information Sharing and Collaboration Program (CISCP), the National Cybersecurity & Communication Integration Center (NCCIC), or the Health Cybersecurity & Communication Integration Center (HCCIC).

2. **Does your organization have an up-to-date inventory of all connected systems in your facilities?**

Healthcare CIOs and CISOs conclude that despite robust attempts to establish an inventory of all connected systems in use within a healthcare organization, most are not as comprehensive as desired, in some cases for reasons outside their control. CIOs and CISOs may routinely discovered devices and applications that were not previously known to be operating on their network. While it may be possible to see every IP address on a network, the owner that is responsible for a device may be unknown, thus a frictional variance of what is accurate and what is known.

Another cause of incomplete inventories is the lack of streamlined procurement of devices, systems and technology across a healthcare organization. While hackers may not care who within the institution purchased they device, the CIOs and CISOs are responsible for securing it regardless of where it came from within the organization.

CHIME and KLAS Research partnered on a medical device cybersecurity benchmarking report in 2018. The report found that the average number of connected medical devices (not broader connected systems per the question) was approximately 10,000. The same study found that of the organizational factors causing medical device security issues, 49 percent cited the lack of an asset inventory or visibility[2].

3. **Does your organization have real-time information on that patch status of all connected systems in your facilities?**

Our members stressed that a real-time patch information loop is nearly impossible. Most members cited they have information about a "point in time," however most would not be aware of a vulnerability and thus a patch, until after a vulnerability scan is complete; in some organizations that run scans 24 hours a day, a need for a patch may not present until 48 hours at the earliest.

The CIOs and CISOs suggested that while real-time patch status may be known for certain devices, it does not exist for many. Our members prefer to categorize this issue as a "up to date" patches rather than "real-time."

One large urban hospital system cited that in June 2016 the system was aware of 600,000 vulnerabilities. The organization has since: launched a concerted effort to improve their cybersecurity posture; expanded their security teams and grown their financial investment in cybersecurity; and has taken their vulnerability count down to about 30,000.

This question does not consider the risks of toppling medical devices that are not able to sustain a vulnerability scan. It also does not acknowledge that in the case of many medical devices, even if organizations are aware of a vulnerability, a patch may either not exist or the health system may not be able to administer it. Further, they may need to wait for the manufacturer to apply the patch. Thus, organizations must be resourceful when it comes to patching. They actively reach out to vendors to find out when patches are available; sometimes they patch devices themselves, and sometimes they have the vendor do it for them. They have also begun requesting that vendors use contract language that clearly outlines patching responsibilities and timelines.

---

[2] Medical Device Security, 2018. What are the Greatest Challenges, and How Can They be Overcome? A KLAS-CHIME Benchmarking Report

4. **How many of your systems rely on beyond end-of-life software and operating systems?**

The 2018 KLAS-CHIME Medical Device Security Benchmarking Report an estimated 33 percent of devices within a healthcare organization are "unpatchable[3]" Anecdotally, our CIOs and CISOs reiterated this with an estimate that in rural health systems the number of devices that could be considered unpatchable or "end-of-life" from a cybersecurity perspective could be higher than 40 percent.

The challenge exists with defining "end-of-life" for the security of the device when the useful life of the device may far exceed its security capabilities. For most healthcare organizations, margins are tight and capital expenditures are established years in advance. The costs associated with deeming a device to be "end-of-life," especially in rural and underserved areas must not be understated. There is often not a direct correlation between cybersecurity end-of-life and useful end-of-life, thus policies must be in place to address the discrepancy. Policymakers must define end-of-life very carefully.

At times there is a lack of transparency relative to the operating systems of medical devices. Efforts have been made on Capitol Hill, as well as, by the FDA, to bring increased transparency following the WannaCry and NotPetya attacks, when wide-spread reports of health systems not having the information available to them to know if their devices were vulnerable to the known threat. The FDA has proposed a cybersecurity bill of materials (CBOM) in their current draft pre-market cybersecurity guidance which we have requested and thus support to bring greater purchaser transparency, as well as in their Medical Devices Safety Action Plan. The FDA further highlighted their CBOM efforts in their Fiscal Year 2020 budget justification.

Our members discuss how often they are forced to buy devices that are close to having software that is considered "end-of-life." Our members believe there should be a requirement to restrict sales of devices with software that is already no longer being supported. Moreover, government should mandate the medical device manufacturers to update software, or if that's not possible, it should be replaced at no cost to the customer.

Our members cite ongoing efforts, and challenges, associated with both managing and mitigating threats stemming from medical devices despite attempts to be more proactive during contract negotiations, as well as, pursuing closer partnerships with manufacturers throughout device lifecycles. Our members highlight that while some of the larger device manufacturers have become more proactive in addressing cybersecurity concerns, smaller manufacturers that offer specialized products struggle mightily. While progress has been made, in large part due to a more proactive stance from the FDA, device security remains both a patient safety and healthcare operations issue. A threat may originate with a device, but the device is part of a much broader ecosystem and that notion has yet to be adopted by medical device manufacturers.

Our recent comments to the FDA in response to the agency's, "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices: Draft Guidance for Industry," may be of interest and can be found here.

It is also worth highlighting that if health systems are forced to trust a conglomeration of open commercial networks to manage their endpoints, we will continue to have an issue securing our medical devices and other critical systems. Unless we have a separate secure system, where trusted parties are vetted securely, as is done with military or other government networks, our medical devices and other end points will still be at risk.

5. **Are there specific steps your organization has taken to reduce its cybersecurity vulnerabilities that you recommend be implemented industry wide?**

[3] Medical Device Security, 2018. What are the Greatest Challenges, and How Can They be Overcome? A KLAS-CHIME Benchmarking Report

Our members recommend the voluntary best practices outlined in question one, as well as seek to highlight the work of the Cybersecurity Act 405(d) task group which resulted in the December 2018 release of "Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients" or HICP.

A deliverable mandated by the Cybersecurity Act of 2015, HICP is a public-private partnership, co-lead by industry and the U.S. Department of Health and Human Services. HICP examines cybersecurity threats and vulnerabilities that affect the healthcare industry. It explores (5) current threats and presents (10) practices to mitigate those threats. In addition to HICP, the task group provided two technical volumes to be leveraged, one for smaller healthcare entities, another for medium to large entities aimed at helping them improve their cybersecurity posture.

CHIME and AEHIS members were actively engaged in the development of HICP and point to it as a valuable, Congressionally-mandated, free resource that organizations can leverage in a manner that best fits their needs and resource constraints. The task group is continuing their work on another volume, and CHIME and AEHIS members stand ready to assist in the effort.

Further, these tools stem from efforts underway by the Healthcare Sector Council's Joint Cybersecurity Working Group which is taking the recommendations made from the Health Care Industry Cybersecurity Task Force report referenced under question #6. CHIME and AEHIS have four members on the executive committee and are very committed to improving our industry's cybersecurity posture.

6. **One of the imperatives from the Health Care Industry Cybersecurity Task Force Report[1] is for the sector to "develop the heath care workforce capacity necessary to prioritize and ensure cybersecurity awareness and technical capabilities." To that end, what workforce and personnel challenges does your organization face in terms of security awareness and technical capacity? What steps have you taken to develop the security awareness of your workforce and/or add or grow technical expertise within your organization?**

Healthcare organizations face a variety of workforce related challenges including but not limited to high turnover rates of nurses and clerks, a shortage of cybersecurity professionals, stretched resources, other sectors poaching cybersecurity talent from healthcare organizations, and executives in smaller and mid-sized organizations holding multiple roles in addition to being charged with security. To address these issues, organizations have adopted a variety of strategies to improve the cybersecurity readiness and hygiene of their organizations by expanding the knowledge base across their enterprises.

To address workforce and personnel challenges, health systems have employed a variety of education initiatives, developing cybersecurity awareness curriculums for the non-information technology workforce. This may include videos and training modules, a focus on social engineering awareness through regular phishing exercises to educate on the dangers of malicious attachments, links or email impersonation. Others hold cybersecurity fairs to cover key topics or themes and capitalize on any opportunity to track and promote a healthy cybersecurity posture. As resources vary by organization, some may only offer videos or posters; most leverage phishing exercises.

Our members are encouraged by efforts to integrate more information technology and cybersecurity training into the nation's medical curriculums. Building cybersecurity awareness and knowledge at the ground level will assist with some of the existing challenges organizations face with their clinicians.

Our CIOs and CISOs detail the challenges with finding cybersecurity talent outside of major metropolitan areas. Organizations struggle to find capable cybersecurity and data analytics professionals and often look to develop talent from within their organization. Some states have leveraged grant programs or loan forgiveness programs to enable health systems to hire and retain qualified talent, but such programs are not ubiquitous.

[1] "Health Care Industry Cybersecurity Task Force," U.S. Department of Health and Human Services (2017), available at: https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf

Congress should consider a federal workforce development program that focuses on healthcare cybersecurity, that could both leverage community colleges and professional certification programs to develop a skilled workforce to combat ongoing workforce shortages in healthcare information security. Additional training could be offered by the Regional Extension Centers (RECs) as was done during the rollout of the EHR incentive program. Additionally, Congress could consider loan forgiveness programs for providing cybersecurity services in the health sector after graduation as some states have done or pursue a program similar to federal service loan forgiveness programs.

7. **Has the federal government established an effective national strategy to reduce cybersecurity vulnerabilities in the health care sector? If not, what are your recommendations for improvement?**

The Health Care Industry Cybersecurity Task Force (HCICTF) report outlined the needs for increased coordination across HHS, unfortunately, to date, this remains elusive. We believe that it is imperative that providers are comfortable relying on HHS as the identified sector-specific agency for assistance and education, without fear that the enforcement actions will follow. This complex paradigm must be addressed.

Just as the industry grapples with finding personnel with cybersecurity expertise and resources to execute a comprehensive cybersecurity program, HHS has similar challenges. Operating divisions within HHS, such as the FDA, have not had dedicated cybersecurity funding, despite it being included in prior budget requests. Further, just as healthcare institutions must coordinate efforts to thwart cyber threats, it is vital that HHS have a coordinated plan to address threats to the data and systems used and housed by the department.

The absence of a national healthcare cybersecurity standard contributes to the frustration and confusion of the industry. Guidance and regulations authored by different operating divisions within HHS run counter to one another. Even the use of “guidance” by some HHS operating divisions versus “regulation” by others leads some in the industry to question whether the guidance is obligatory or optional. The Office for Civil Rights (OCR) is focused on HIPAA compliance, which as we will outline below, does not necessarily equate to good cybersecurity alone. As stated above, most healthcare organizations leverage the NIST CSF, but it does not get into the level of detail that OCR expects.

As an example, the FDA and OCR should align their guidance and enforcement activities to ensure that medical devices are compatible with the requirements for safeguarding protected health information (PHI) as required by providers, their business associates (Bas), and other covered entities regulated under the Health Insurance Portability and Accountability (HIPAA), as well as, the breach requirements outlined for these parties under the Health Information Technology for Economic and Clinical Health Act (HITECH). As integral partners in the healthcare ecosystem, medical devices manufacturers must share responsibility for safeguarding patient data which if compromised via cyberattack can also create risks to patient safety. Today, not every medical device manufacturer has signed business associate agreements (BAAs) as required under HIPAA, with providers. Further, we have fielded many reports from members about some device manufacturers having access to PHI, yet they do not hold a BAA with the provider despite requests to sign one.

The absence of a coordinated healthcare cybersecurity strategy is only compounded by the lack of federal investment. Congress must allocate the necessary resources to enable the entire healthcare ecosystem to allow for the expeditious delivery of solutions to meet the imperatives set forth in the HCICTF report.

8. **Are there specific federal laws and/or regulations that you would recommend Congress consider changing in order to improve efforts to combat cyberattacks on health care entities?**

To offer an overarching recommendation for your consideration, as patient health data becomes digital and more fluid, we must ensure the implementation of stringent privacy and security standards. As we increase interoperability, additional threats to data integrity will arise. Without proper safeguards, the safe and

secure transmission of sensitive data will continue to be a challenge and will hinder efforts to care outcomes. And, this extends well beyond medical devices.

Specifically, the complexities with meeting HHS privacy and security requirements can be staggering. Audits by OCR are perceived as being punitive and not assisting the organization to recover and learn from a breach. Providers today must dedicate highly valuable resources to navigate a complex and often unbalanced and punitive regulatory landscape. Resources and efforts are often focused on compliance with OCR requirements, which may not always represent the greatest threats faced by a healthcare provider, diminishing rather than aiding their ability to guard PHI.

It is vital that Congress and HHS identify a pathway for ensuring providers do not unduly shoulder the burden of protecting PHI in situations outside their control. To further enhance proactive collaboration, safe harbors from Resolution Agreements as an incentive for organizations that demonstrate, and certify, cybersecurity readiness should be offered, which may warrant Congress to amend provisions of the HITECH Act. This will encourage the investment into cybersecurity from the providers in an age when it is understood no organization can prevent all cybersecurity attacks. Further, it may be necessary for Congress to consider revising some of the definitions set forth in HITECH, such as the definition of a breach, as to not presume guilt.

HHS must start by offering providers better guidance for assessing threats that they can control as opposed to those that are out of their domain. Additionally, OCR should acknowledge and recognize provider efforts and investments to safeguard information and information systems when assessing the scope and magnitude of enforcement actions. For instance, HHS should be encouraged to pursue policies which reward providers and other covered entities for engaging in good faith efforts to prevent cybersecurity attacks rather than being unduly punitive. An example of this would be demonstrating sufficient compliance NIST's CSF or working to meet best practices such as those co-developed by HHS and in industry like HCIP. Providers must be able to maximize protections allowed BAAs by redistributing responsibility for security more evenly among covered entities and their BAs.

Additionally, the HCICTF Report includes an entire section (page 35) that discusses the myriad of issues associated with the anti-kickback and Stark statutes. The report says:

> *A regulatory exception to the Stark Law and a safe harbor to the Anti-Kickback Statute to protect certain donations of electronic health records (EHR) effectively addresses management of technology between health care entities and serves as a perfect template for an analogous cybersecurity provision. Physician groups confront a myriad of financial challenges. Often these financial constraints limit their ability to manage the EHR software without trained security professionals who have the expertise to provide sufficient cybersecurity programs to protect their patient records. We need to empower small providers or suppliers (e.g., physician practices) to actively manage their security posture, not hinder them. Often organizations want to provide technology to ensure smaller business partners do not become a liability in the supply chain. An exception may provide for this assistance without creating fear of violating the Stark Law or Anti-Kickback Statute.*

Based upon the recommendations from the HCICT report and the need identified by many of our members, we strongly believe an exemption to the Stark and Office of Inspector General (OIG) Antikick statutes that permits for donations of services that further an entity's cybersecurity posture is warranted. We recognize there may be limitations around how such an exemption is crafted; however, if it followed many of the requirements that the CMS and OIG have laid out around the exceptions permitted for donating an EHR, this would be helpful. Ideally, we recommend that HHS exemptions / safe harbors to permit donations of training / education services, software and technology. Technologies with the greatest impact on improving cybersecurity hygiene, as identified by CIOs and CISOs, include: firewalls / intrusion detection and

prevention systems, antivirus / malware, email filtering / encryption, data loss prevention software, and advisory services.[4]

There is an opportunity to better identify and reduce cybersecurity vulnerabilities associated with biomedical equipment used in the healthcare sector. Vulnerabilities in a general purpose (non-bio-medical) commercial system, such as an application or operating systems, are typically identified by academia, federal or industry partners. These vulnerabilities are often not applicable or carry a lower severity for cybersecurity threats since the underlying operating system in biomedical equipment is highly tailored or in a controlled environment. However, the process of making such a determination is resource intensive and involves close coordination with each product vendor.

To put this challenge in perspective, one member at a children's hospital has deployed over 1,000 networked biomedical devices manufactured by dozens of different vendors. When multiplied by the hundreds of potentially critical vulnerability announcements made each year, the vulnerability management of biomedical equipment quickly becomes a non-scalable problem. Historically, the health system has observed the time to respond from vendors impacted by vulnerabilities has been insufficient to address operational risks to the healthcare organization. Ss noted earlier, this includes patch releases and/or mitigation recommendations. The regulatory requirements with HIPAA and HITECH generally result in the cybersecurity risk of such a vulnerability being borne by the healthcare organization. There could be an opportunity to have this risk more equally shared by the biomedical equipment manufacturers and the healthcare organization through regulatory means or enhanced FDA oversight for deployed devices. This could result in a more comprehensive vulnerability management condition for these types of equipment.

Congress must pursue an expansion of FDA's current authority to enable them to take a more proactive stance in addressing medical device cybersecurity. The security of a device must be considered when evaluating the safety and efficacy of its performance, and per the FDA's FY20 budget justification, additional authority is necessary.

> *Currently, there is no statutory requirement (pre- or post-market) that expressly compels medical device manufacturers to address cybersecurity. This proposal would advance medical device safety by ensuring FDA and the public have information about the cybersecurity of devices. Specifically, FDA seeks to require: that devices have the capability to be updated and patched in a timely manner; that premarket submissions to FDA include evidence demonstrating the capability from a design and architecture perspective for device updating and patching; a phase-in approach to a Cybersecurity Bill of Materials (CBOM), a list that includes but is not limited to commercial, open source, and off-the-shelf software and hardware components that are or could become susceptible to vulnerabilities; and that device firms publicly disclose when they learn of a cybersecurity vulnerability so users know when a device they use may be vulnerable and to provide direction to customers to reduce their risk. The proposal also seeks to improve proactive responses to cybersecurity vulnerabilities.*[5]

Congress in conjunction with the FDA should ensure that manufacturers configure their devices according to an industry accepted security standard that accounts for the basic principles of cybersecurity controls and alleviates risks. Manufacturers should, as part of the pre-market approval process, be required to undergo a level of security validation in order to provide healthcare providers with a very simple and easy to implement mechanism for managing its security. The FDA must institute a clear enforcement process for reporting cybersecurity vulnerabilities that remain unaddressed by manufacturers. The FDA should provide safe-harbor protections to manufacturers that follow the FDA's post market guidance on device cyber

---

[4] KLAS, "Cybersecurity 2017 Understanding the Healthcare Security Landscape, "February 2017 Performance Report, https://klasresearch.com/report/cybersecurity-2017/1121.

[5] DEPARTMENT of HEALTH and HUMAN SERVICES Food and Drug Administration Fiscal Year 2020 Justification of Estimates for Appropriations Committees https://www.fda.gov/downloads/AboutFDA/ReportsManualsForms/Reports/BudgetReports/UCM633738.pdf

security assuming this is tweaked to include the aforementioned level of security validation , and penalties for manufacturers that fail to abide by the guidance in regard to "uncontrolled risks," a term created by the FDA to signify cybersecurity risks pose risks to patient safety and have caused known adverse events or deaths. Further, our members believe the FDA should pursue a systematic way for collecting information on cybersecurity vulnerabilities. Finally, a process is needed to ensure that when a risk is determined to be "controlled," a term used by FDA to signify a risk where there are no known adverse events. Our members report some manufacturers deem risk to be controlled despite disagreement by the provider; today there is little recourse to have this changed.

9. **Are there additional recommendations you would make in establishing an industry wide strategy to improve cybersecurity in the health care sector?**

CHIME and AEHIS members point again to the HICP document as a resource for industry best practices to establish an industry-wide strategy. Just as HICP was a public-private partnership between HHS and industry, it is vital that HHS serve as the resource the industry is in dire need of. We encourage HHS to continue to play an active role in future iterations of HICP as well as to explore other opportunities for industry collaboration.

Not only is government partnership necessary, as outlined above, resources and incentives must be considered. Whether there is the need to replace "end-of-life" devices, hire skilled cybersecurity personnel or implement a comprehensive cybersecurity strategy, more resources are a necessity. While monetary assistance would be welcome, Congress, along with the administration, must consider additional incentives to better aid healthcare providers. Other incentives could include a safe harbor from OCR penalties if providers are following the HICP (or other cybersecurity best practices) or a Merit-based Incentive Payment System (MIPS) improvement activity for eligible providers to implement a robust cybersecurity program. HHS must reconsider their breach reporting standard, as outlined above, to focus on processes and outcomes that will improve a provider's cybersecurity posture, not be strictly compliance focused.

Further, we reiterate the need to develop a qualified workforce. Efforts are necessary to re-enforce learning that promotes engineering thought processes, and other STEM (Science Technology Engineering Mathematics) skills at an early age.

Congress should also consider legislation that protects well intentioned security researchers. Independent researchers are discovering new vulnerabilities, and some have been prosecuted. Creative vulnerability seeking individuals should be cultivated rather than restrained. If future wars will be cyberwars, this is a skill set that will be needed for the defense of the nation. As you are likely aware, Department of Homeland Security (DHS) Secretary Kirstjen Nielsen recently delivered a speech at DHS's Science and Technology Directorate's Cybersecurity and Innovation Showcase where she highlighted the barrage of threats the U.S. is facing from foreign adversaries.

CHIME and AEHIS commend your willingness to engage stakeholders in an effort to pursue policies to improve cybersecurity in healthcare. We hope our comments are useful and look forward to a continued dialogue with your staff about how we can better protect patients and their sensitive healthcare data. Should you have any questions or if we can be of assistance, please contact Leslie Krigstein, Vice President of Congressional Affairs at *lkrigstein@chimecentral.org*.

Sincerely,

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

Sean Murphy
Chair, AEHIS Advisory Board
Chief Information Security Officer
Premera Blue Cross