November 14, 2022

The Honorable Jennie M. Easterly
Director, Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security
245 Murray Lane SW
Washington, DC, 20528

Dear Director Easterly:

On behalf of the Healthcare Information and Management Systems Society (HIMSS), we are pleased to provide comments in response to your Request for Information (RFI) on the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). HIMSS appreciates the opportunity to leverage our members' expertise to share feedback on this critical topic, and we look forward to continued dialogue with you and the Department of Homeland Security (DHS) on the implementation on this law as we all continue to help protect our critical infrastructure.

HIMSS is a global advisor and thought leader supporting the transformation of the health ecosystem through information and technology. As a mission-driven non-profit, HIMSS offers a unique depth and breadth of expertise in health innovation, public policy, workforce development, research, and analytics to advise global leaders, stakeholders, and influencers on best practices in health information and technology. Through our innovation engine, HIMSS delivers key insights, education and engaging events to healthcare providers, governments, and market suppliers, ensuring they have the right information at the point of decision. Headquartered in Chicago, Illinois, HIMSS serves the global health information and technology communities with focused operations across North America, Europe, the United Kingdom, the Middle East, and Asia Pacific. Our members include more than 130,000 individuals, 480 provider organizations, 470 non-profit partners, and 650 health services organizations.

HIMSS is pleased to provide input in response to this RFI, as the Cybersecurity and Infrastructure Security Agency (CISA) begins to develop and oversee implementation of regulations for critical infrastructure sectors, including healthcare, to submit reports detailing covered cyber incidents and ransom payments. We believe the following areas are especially important for CISA to consider when creating the policies and provisions related to mandatory cybersecurity information sharing:

1. **Reducing Reporting Redundancy:** The granularity of data that must be reported must be balanced against what is already mandated under existing laws (e.g., the Health Insurance Portability and Accountability Act (HIPAA)), and any future federal reporting requirements. To reduce administrative burden and costs, any mandatory reporting of covered cyber incidents should occur only once to a single federal agency instead of having to report the same covered incident to multiple federal agencies.
2. **Balanced Reporting Requirements:** Data reporting requirements should be balanced and factor in the following considerations:

a. Minimize data reporting to only what is necessary and, on a need, to know basis;
b. "Covered entities" (yet to be defined) in the healthcare critical infrastructure sector should only be required to report details after assessing the actual scope and impact of the incident, taking bona fide steps to contain the incident, and undertaking reasonable mitigation efforts;
c. Data reporting should be tailored to sector-specific needs and requirements;
d. CISA should proactively work with partner federal agencies to define the single process for reporting purposes;
e. Federal agencies should collaborate and coordinate if an incident is reported outside of CISA, to avoid shifting/adding reporting burdens and costs for healthcare stakeholders. As part of the coordination, reporting should occur only once and in a manner that is consistent with the scope and spirit of CIRCIA
f. In the near term, encouraging entities to report their data using standard protocols (e.g., STIX/TAXII or otherwise) should be encouraged but not mandated where infeasible to accommodate smaller healthcare facilities with limited cybersecurity resources and staff;
g. Indicators of compromise, tactics, techniques, procedures, and best practices should be shared in a timely and expedient manner to reduce the risk of a cyber incident propagating within the healthcare sector and across other critical infrastructure sectors and
h. CISA should partner with sector specific ISACs, ISAOs, and affiliated organizations for continued guidance and feedback regarding what types of information and deliverables are useful to critical infrastructure stakeholders, which may vary from sector to sector

3. **Granularity of reporting:** Various healthcare organizations, including but not limited to small and medium healthcare stakeholders, may not necessarily have the resources to report granular data or within relatively short timeframes as required by CISA. Such organizations may require additional assistance from CISA and other federal agencies to enhance their reporting processes and should not be penalized if they are attempting to comply with CIRCIA requirements in good faith CISA and HHS should work together to continue finding ways for shared services or mutual aid arrangements between well-resourced and limited-resourced organizations.

4. **Confidential handling and protection of Reported Information:** It is vital to require confidential handling and protection of the reported information considering national security concerns to protect the nation's critical infrastructure and constituent entities. Such information should also be exempt from FOIA. Otherwise, the release of such information, in whole or in part, may provide a "roadmap" for attackers and other bad actors to compromise organizations and infringe upon our national security.

Definitions and Applicability

Healthcare stakeholders are under constant attack and are fending off relentless cyberattacks daily. HIMSS believes it would overwhelm our sector, as well as CISA, if covered entities were required to report to CISA cyber incidents other than ones designated as "substantial." Therefore, we strongly recommend that CISA: 1) only require that "substantial" events be required to be reported and namely those events that either have the potential to jeopardize national security or events that are a direct threat to patient safety (such as a ransomware attack); 2) that healthcare stakeholders have the sole discretion to assess whether an incident is indeed a "substantial cyber incident"; and 3) should healthcare stakeholders determine -- after a review that exceeds 72 hours -- that a cyber incident is, indeed, "substantial" – that reporting it within a reasonable timeframe thereafter is permitted, and should not result in any penalization or adverse consequences for such stakeholders. Such delays may be for good faith reasons such as, but not limited to: (i) the need to further investigate an incident to truly assess the scope and impact of said incident, (ii) any reasonably necessary mitigations to address the incident, and (iii) any delays due to the involvement of law enforcement.

Additionally, we seek clarification from CISA on whether not-for-profit entities will be subject to mandatory cyber reporting requirements. CIRCIA defines a "covered entity" to be, "an entity in a critical infrastructure sector, as defined in Presidential Policy Directive 21, that satisfies the definition established by the Director in the final rule issued pursuant to section 2242(b)." According to Presidential Policy Directive 21, this includes public and private entities. Given that most hospitals and healthcare delivery organizations (HDOs) are not-for-profit entities, we would appreciate clarification from CISA on whether such not-for-profit entities are deemed to be private entities, and thus subject to the mandatory cyber reporting requirements.

Data Reporting

In considering what essential elements of information must be reported to CISA, HIMSS recommends that the agency consider several factors:

1. Data reporting requirements should be limited to include only what information is necessary on a need-to-know basis and within the scope and spirit of CIRCIA, including regarding sharing, in a timely and expedient manner, indicators of compromise, tactics, techniques, procedures, and best practices to reduce the risk of a cyber incident propagating within the healthcare sector and across other critical infrastructure sectors.
2. Healthcare stakeholders, like many other critical infrastructure stakeholders, are typically not able to accurately attribute a cyber incident to a nation state or non-state sponsored attack. (Rather, this is the province of agencies such as the Federal Bureau of Investigation, the National Security Agency, and their partner organizations.) "Covered entities" (yet to be defined under the statute) in the healthcare critical infrastructure sector should only be required to report details after assessing the actual scope and impact of the incident, taking bona fide steps to contain the incident, and undertaking reasonable mitigation efforts. It is also important to note that an entity may not necessarily know which vulnerabilities may have been exploited at the time of the first report to CISA about

the cyber incident. In the spirit of information sharing, CISA should consider allowing additional reports about the cyber incident, should the healthcare stakeholder become aware of such additional information. The kind of information to be relayed depends upon what is happening, such as additional (but related) compromises that may transpire or additional information may be gleaned after further investigation about the cyber incident that was first reported

3. Data reporting should be tailored – when necessary – to sector-specific needs. For example, some healthcare stakeholders may be unfamiliar with cyber threat information sharing and collecting said information. Certain healthcare stakeholders also may not yet have the capabilities to detect and monitor networks and systems for potential incidents.
4. CISA should proactively work with partner federal agencies to define the "front door." If CISA expects reporting within 72 hours, we believe it should also be CISA's responsibility to notify other federal authorities like the FBI, unless such authorities have already been notified by the impacted stakeholder. But, just the same, we also expect CISA to allow for reasonable delays, whether: (i) requested by law enforcement or (ii) as necessary for reasonable mediation efforts and (iii) as necessary for reasonable investigation efforts.
5. If reporting is made to a federal agency other than CISA, then it should be incumbent on that federal agency to share the threats with CISA without shifting the burden and adding additional costs for healthcare stakeholders; penalizing healthcare stakeholders in these situations should be avoided.
6. Regarding sharing reported information with other stakeholders within the healthcare sector and with other critical infrastructure sectors, the type of information that is consumable and usable by other stakeholders (whether within the healthcare sector or across other critical infrastructure sectors) may vary, depending upon the sector. Some critical infrastructure sectors are more mature than others. Indicators of compromise, tactics, techniques, procedures, and best practices should be shared in a timely and expedient manner to reduce the risk of a cyber incident propagating within the healthcare sector and across other critical infrastructure sectors. Healthcare stakeholders include, but are not limited to, all sizes of healthcare providers, payers, pharmaceutical/life sciences organizations, medical device manufacturers and other third-party vendors and suppliers.
7. Notwithstanding the foregoing, CISA should clarify which information handling caveats to be associated with the information that is to be disseminated for the benefit of other stakeholders, whether in the healthcare sector or with other critical infrastructure sectors. HIMSS recognizes that some information may be restricted to: (i) certain individual recipients, (ii) the organization itself, (iii) limited on a need-to-know basis for sharing with the organization and its respective clients, (iv) within the community, and/or freely shared with the world. Furthermore, in light of threats to national security and threats by nation-state and non-state actors and other special circumstances requiring sensitive handling of information, it is recognized that certain information should only be shared within certain boundaries (and, sometimes, within national boundaries). Nonetheless, it is also recognized that cyber-attacks can occur transnationally, including from west to east or east to west and it is also important to appropriately ensure information sharing amongst trusted information sharing partners, when warranted.

8. Encouraging entities to report their data using standard protocols (e.g., STIX/TAXII or otherwise), but only when feasible. This will enable automated indicator sharing.
9. CISA should partner with sector specific ISACs, ISAOs, and affiliated organizations for continued guidance and feedback regarding what types of information and deliverables are useful to critical infrastructure stakeholders, which may vary from sector to sector. It is well known that threat actors use many of the same – or substantially similar -- tactics, techniques, and procedures and therefore it is vital to have both intra-sector (in this case, within the healthcare sector) and cross-sector information sharing. Furthermore, the healthcare sector is unique in that it depends upon virtually all other critical infrastructure sectors and so it is especially vulnerable. CISA should work with ISACs, ISAOs, and affiliated organizations for continued guidance and feedback regarding how we can efficiently share cyber threat and mitigation information with all relevant stakeholders.
10. CISA should define any information, services and/or support that may be made available from CISA to the covered entity in response to the incident report. CISA should also clarify whether it is mandatory or voluntary for stakeholder organizations to adopt any recommended guidelines, best practices, and/or processes that CISA may have considering said incident report.

Avoid Duplicative Reporting

HIMSS has long supported the need for stronger information sharing practices. While the Cybersecurity Information Sharing Act of 2015 took a big step by providing a means for voluntary cyber threat information sharing, many healthcare stakeholders and other critical infrastructure sectors are hesitant to share such information, whether due to concerns about reputational harm or otherwise. It is therefore important to protect the confidentiality of the information that is shared and to robustly protect this information so that the victim organization is not unnecessarily exposed. But we also believe it is imperative for cyber threat information to be quickly and expediently shared with others so that healthcare stakeholders can focus on the coordination and delivery of high-quality care and protect the safety of patients. Nonetheless, HIMSS believes that to the degree possible, any duplicative reporting that is currently required under other Federal policies should be avoided.

Under CIRCIA, CISA does not require reporting from a covered entity where that covered entity is already required by law, regulation, or contract to report substantially similar information to another Federal agency within a substantially similar timeframe, we ask that CISA consider the extent to which its reporting requirements may be harmonized with those of the United States Department of Health and Human Services (HHS) Office for Civil Rights (OCR) and the Federal Trade Commission (FTC) such that a given incident need only be reported to a single federal agency (i.e., only once).

The healthcare industry is already required to comply with a myriad of state and federal cyber, security, and privacy data breach reporting requirements. These include federal authorities and requirements under HIPAA regulations and the Health Information Technology for Economic and Clinical Health (HITECH Act) regulations. Specifically, the HIPAA Breach Notification Rule, as well as the HITECH Act's additional data breach reporting requirements to HHS OCR, and the FTC's Health Breach Notification Rule. At the

state-level, in 2021, at least 45 states and Puerto Rico introduced or considered more than 250 bills or resolutions that deal significantly with cybersecurity; and at least thirty-six states enacted bills in the same year. So far in 2022, at least 40 states and Puerto Rico introduced or considered more than 250 bills or resolutions that deal significantly with cybersecurity; and twenty-four states enacted at least 41 bills in 2022.

As stated earlier, HIMSS would also appreciate significant consideration and clarification in the proposed rulemaking regarding the intersection of the potential future proposed rule regarding "Mandatory Cyber Incident Reporting" and existing federal and state laws, regulations, and oversight. We strongly recommend that DHS and CISA coordinate with other federal agencies with existing jurisdiction – including HHS, HHS OCR, and the FTC – to ensure that duplicative cyber incident reporting requirements are avoided to the greatest extent possible. We strongly urge CISA to leverage existing federal and state cyber incident and data breach reporting requirements for consistency and to reduce the burden on covered entities.

CISA states that they are "particularly interested in input on definitions for and interpretations of the terminology to be used in the proposed regulations; the form, manner, content, and procedures for submission of reports required under CIRCIA; information regarding other incident reporting requirements including the requirement to report a description of the vulnerabilities exploited; and other policies and procedures, such as enforcement procedures and information protection policies, that will be required for implementation of the regulations." We strongly urge CISA to host a series of stakeholder meetings to garner feedback from the healthcare industry, specifically, before promulgating a proposed rule. It is critical that the proposed regulations do not inadvertently create overly duplicative requirements, penalize healthcare stakeholders unfairly, and add burden to an already highly regulated sector of our critical infrastructure. HIMSS and our members welcome the chance to serve as a resource to CISA throughout this process.

In addition, HIMSS requests that CISA allow for a delay in reporting under CIRCIA in instances where "covered entities" in the healthcare critical infrastructure sector are already working with law enforcement or as otherwise requested by law enforcement. For example, HIPAA allows for a reporting delay if a law enforcement official indicates that a notification, notice, or posting required under HIPAA would impede a criminal investigation or result in harm to national security. Covered entities (as defined under HIPAA) may disclose protected health information (PHI), without the individual's authorization, to a public health authority acting as authorized by law in response to a bioterrorism threat or public health emergency. The HIPAA Privacy Rule also permits a covered entity to disclose protected health information to public officials who are reasonably able to prevent or lessen a serious and imminent threat to public health or safety related to bioterrorism to avert a serious threat to health or safety. In addition, disclosure of PHI, without the individual's authorization, is permitted where the circumstance of the emergency implicates law enforcement activities. If CISA promulgates rulemaking that fails to allow a law enforcement delay for notification by law enforcement, it would result in a direct conflict with the reporting requirements under HIPAA and the FTC Breach Reporting Rule. Furthermore, it could undermine the efforts of law enforcement, HIPAA, and increase the risk of harm to the covered entity, the overall

healthcare industry, impacted individuals, state and/or federal investigations, and national security.

HIMSS requests clarification on whether CIRICIA has any extraterritorial reach or whether CIRCIA solely applies to "covered entities" that are situated within the United States.

Further, HIMSS also requests that CISA issue guidance on how "covered entities" under CIRICIA – including healthcare stakeholders – can comply with the requirements of EU GDPR. While not every healthcare stakeholder is required to comply under EU GDPR, some are required to comply considering the extraterritorial reach of EU GDPR.

Prioritize Patient Safety

Patient safety in the healthcare sector means not just ensuring access to care but ensuring that patient safety is not jeopardized. Adding an additional requirement to provide detailed reporting of all the vulnerabilities exploited during a significant incident should not be prioritized over patient safety. Therefore, considerations should be given to the 72-hour reporting mandate and what precisely is required during this period, when a healthcare stakeholder is appropriately prioritizing and triaging patients during this impacted window.

Extreme Events

Cyber incidents can happen at any time to virtually any entity. Sometimes, cyber incidents may happen during inopportune times. For example, a healthcare stakeholder may be experiencing a hurricane, flood, fire, earthquake, or other natural disaster or an extreme event (e.g., terrorism, nuclear, chemical, or biological incidents, , etc.). Extreme events such as these would necessarily warrant a reasonable extension to the otherwise required 72-hour reporting mandate. Additionally, as evidenced by the COVID-19 pandemic, pandemics can indeed cause delays in reporting (and other normal operations) depending upon the circumstances.

Small and Lesser-Resourced Stakeholders

Many healthcare stakeholders are under-resourced, and some do not even have a single, full-time employee devoted to day-to-day cybersecurity operations, even as threats have escalated year after year. With the health sector only as strong as its weakest link, it is imperative that CISA prioritize assisting smaller and lesser resourced stakeholders in fending off growing and sophisticated attacks aimed at stealing intellectual property, extorting ransoms, and otherwise interfering with normal business and clinical operations of healthcare stakeholders.

Mutual Aid

It is not uncommon for some healthcare stakeholders to have mutual aid agreements with each other. For example, a hospital that is unable to take care of patients may have an existing agreement with a nearby hospital (or hospitals) to take care of patients that need to be diverted.

Additionally, certain healthcare stakeholders have mutual aid agreements which extend to cyber incidents (such as, but not limited to, ransomware attacks). CISA could greatly benefit the healthcare critical infrastructure sector and other sectors by standing up a mutual aid network of resources upon which entities that need assistance can enlist assistance from a trusted and vetted entity (whether a peer organization or otherwise).

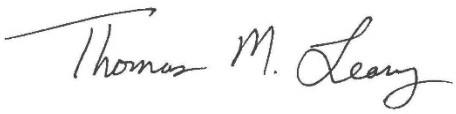
Prioritize Education

HIMSS supports CISA's wide range of resources and the Shields Up program – including cybersecurity assessments that evaluate operational resilience, cybersecurity practices, organizational management of external dependencies, and other key elements of a robust and resilient cyber framework. These professional, no-cost assessments are provided upon request on a voluntary basis and can help any organization with managing risk and strengthening the cybersecurity of our Nation's critical infrastructure. The ability to rapidly respond to cybersecurity incidents – and when possible, preventing them – while sharing information with our federal partners is essential to protect hospitals and healthcare delivery organizations.

HIMSS appreciates the opportunity to comment on the CISA RFI. As CISA continues to garner input from the public in developing proposed regulations required by CIRCIA, HIMSS and our members would appreciate continued opportunities to help inform the important work being done by CISA. We look forward to continuing to be a trusted stakeholder and resource to you and welcome the opportunity to discuss these issues with you and the department. We would be happy to facilitate discussions between your staffs and HIMSS members with unique subject matter expertise on these topics. Please feel free to contact, Eli Fleet, Director, Government Relations, with questions or for more information.

Thank you for your consideration.

Sincerely,



Thomas M. Leary
Senior Vice President & Head of Government Relations