EHNAC

**Electronic Healthcare Network Accreditation Commission**

**www.EHNAC.org**

**Lee B. Barrett**
*Executive Director*

**Debra C. Hopkinson**
*Operations, VP*
*Dhopkinson@ehnac.org*

September 9, 2016

EHNAC
25 Brookshire Lane
Farmington, CT  06032

Nakia Grayson
National Institute of Standards and Technology
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899

**RE: Document Citation 81 FR 52827**

The Commission will make detailed recommendations to strengthen cybersecurity in both the public and private sectors, while protecting privacy, ensuring public safety and economic and national security, fostering discovery and development of new technical solutions, and bolstering partnerships between Federal, State, and local government and the private sector in the development, promotion, and use of cybersecurity technologies, policies, and best practices. According to the Executive Order, the Commission's recommendations should address actions that can be taken over the next decade to accomplish these goals.

# Input to the Commission on Enhancing National Cybersecurity

The response to this RFI is provided by the Electronic Healthcare Network Accreditation Commission (EHNAC). Founded in 1993, EHNAC is an independent, federally recognized, standards development organization and tax-exempt, 501(c)(6) non-profit accrediting body designed to improve transactional quality, operational efficiency and data security in healthcare.    From the experience of EHNAC has as an accrediting organization, information security in healthcare has improved over the last 20 years, thanks to the attention paid to identifying and remediating weaknesses

**□ Critical Infrastructure Cybersecurity**

Challenges and Approaches

1. Current and future trends and challenges in the selected topic area;

In its infancy, electronic communication was fraught with challenges of remediating weaknesses in a fairly new technology. Discovery of weaknesses have led to the strengthening of infrastructure over time. It is expected that as new technologies are introduced, new weaknesses and vulnerabilities will be discovered in the future and remediation will take place. The largest challenge is to identify and remediate those weaknesses as soon as possible before they have the opportunity to be heavily exploited.

2. Progress being made to address the challenges;

One of the more prominent ways the challenges are being addressed is through accreditation or certification of software systems, network infrastructure, and general business practices. EHNAC provides such services to organizations such as healthcare clearinghouses, financial lockbox facilities, practice management systems, and outsourcing organizations that primarily act as Business Associates as defined by the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Because EHNAC has the advantage of reviewing many organizations, best practices have evolved over time and the most prominent and widely used with strongest value of those practices becomes the baseline for the accreditation programs being implemented.

3. The most promising approaches to addressing the challenges;

   The most promising approach to addressing the challenges is for organizations implementing an infrastructure strategy to leverage the best practices of third party accrediting organizations such as EHNAC and to validate those strategies through self-assessment and review by an independent third party. It is not enough for an organization to implement the strategy on their own because experience has shown that organizations tend to take a "that's good enough" approach to security, policies and procedures documentation, and monitoring and reporting of incidents. Having a third party review those critical areas aid in the identification and remediation of gaps within such strategies.

4. What can or should be done now or within the next 1-2 years to better address the challenges;

   - Increasing education for healthcare organizations of all types related to the best practices in securing electronic data.
   - Increase the requirements related to third party accreditation or certification for vendors and users of healthcare software.

5. What should be done over the next decade to better address the challenges; and

   By the end of the decade, vendors and users of healthcare software should be held accountable to a baseline set of best practice requirements to enhance the overall security of electronic data being exchanged in healthcare through independent third party accreditation or certification.

6. Future challenges that may arise and recommended actions that individuals, organizations, and governments can take to best position themselves today to meet those challenges.

   Future challenges will include the continuous identification of vulnerabilities, especially as new technologies are introduced however, as long as organizations that have exposure to a large number of systems, strategies and data exchange are able to get out in front of the issues and share that information through accreditation programs such as EHNAC's, the baseline best practices will continue to improve as necessary.

<u>Additional Information</u>

1. Emerging technology trends and innovations; the effect these technology trends and innovations will have on the digital economy; and the effect these technology trends and innovations will have on cybersecurity.

Since the inception of EHNAC, many trends have developed in the way of cybersecurity. Transmission of lightly secured healthcare files to insurance company bulletin board systems have given way to heavily secured and encrypted file transfer methods. Office-based server rooms have given way to independently run datacenters and cloud service providers. By bundling the customer base into common facilities, and infrastructure, organizations will be able to save money and focus workforce on securing the data versus securing the facility.

2. Economic and other incentives for enhancing cybersecurity.

   HIPAA alone has instituted penalties for the inappropriate disclosure of Protected Health Information (PHI). The penalties could result in an organization paying hundreds of thousands if not millions of dollars in fines if the data to which they are entrusted is not appropriately safeguarded. Such fines provide enough incentive to organizations to ensure their cybersecurity framework is in place and effective. Public awareness of threats and breaches is also providing incentives for organizations to protect themselves.

3. Government-private sector coordination and cooperation on cybersecurity.

   EHNAC has been working with various government entities to provide insight into the issues being discovered through accreditation efforts. EHNAC regularly consults with the Office of the National Coordinator (ONC), the Office for Civil Rights (OCR), Veterans Administration (VA), and more, in an effort to share information and provide guidance as to best practices in protecting electronic healthcare information. Government entities should consider using EHNAC accreditation processes to assure their own protection against cyber threats.

4. The role(s) of the government in enhancing cybersecurity for the private sector.

   EHNAC believes it is important for the government to provide feedback on best practices and support independent third party accreditation and certification for organizations to enhance cybersecurity for vendors of healthcare software.

5. Performance measures for national-level cybersecurity policies; and related near-term and long-term goals.

   Measure compliance with OCR audits, EHNAC accreditations, and ONC certifications resulting in a report to highlight areas of highest frequency of weakness versus highest frequency of compliance so such policies may be adjusted in the weakest areas discovered. Goals may be established once a baseline compliance is determined.

6. Complexity of cybersecurity terminology and potential approaches to resolve, including common lexicons.

   Incorporate a glossary of terms or wiki that allows for updates from knowledgeable individuals with citations.

□ **Cybersecurity Workforce**

<u>Challenges and Approaches</u>

1. Current and future trends and challenges in the selected topic area;

   Enhanced policies, procedures, and education are all areas that are trending to the positive as it relates to cybersecurity workforce. Workforce members may sometimes be starved for such information or knowing where to find it. Challenges such as that appear to mostly affect the smaller vendors of healthcare software and start up organization's because such infrastructure is not always put in place in the beginning.

2. Progress being made to address the challenges;

   Progress is being made to address the challenges by utilizing third party consultants or accrediting organizations to focus on those activities and ensure that complete policies, procedures, and education opportunities are readily available to workforce members. Security reminders are being implemented on a more consistent basis among healthcare organizations.

3. The most promising approaches to addressing the challenges;

   Organizations have access to online resources now more than any other time in the past. Online education tools allow for up-to-date information to be shared with workforce members and typically includes testing at the end of the session as well as tracking and reporting of compliance among workforce members. HIPAA training and security awareness training all provide for at least annual review of changes to policies, procedures, and best practices related to cybersecurity.

4. What can or should be done now or within the next 1-2 years to better address the challenges;

   Continue to evaluate compliance of policies, procedures, and education through independent third party accreditation.

5. What should be done over the next decade to better address the challenges; and

   The government and private industry should consider developing a standard set of training materials for non-technical workforce members. By the end of the decade, vendors of healthcare software should be held accountable to maintaining a comprehensive set of policies, procedures, and education for workforce members. Validation of such compliance may be conducted through independent third party accreditation efforts.

6. Future challenges that may arise and recommended actions that individuals, organizations, and governments can take to best position themselves today to meet those challenges.

   Future challenges may include additional legislation on the healthcare vendors that will require more stringent assessment of current policies, procedures, and education needs. Utilizing third party tools to monitor and incorporate updates to policies, procedures, and education materials will aid an organization in compliance efforts. Utilizing a third party accreditation provides the additional validation that best practices are being satisfied.

Additional Information

1. Emerging technology trends and innovations; the effect these technology trends and innovations will have on the digital economy; and the effect these technology trends and innovations will have on cybersecurity.

   As noted previously, online tools provide for a simple and inexpensive way to ensure compliance with new trends related to cybersecurity.

2. Economic and other incentives for enhancing cybersecurity.

   By providing information at the fingertips of workforce members, organizations are better able to avoid inappropriate disclosures of PHI as well as manage the infrastructure that supports the PHI.

3. Government-private sector coordination and cooperation on cybersecurity.

   EHNAC has been working with various government entities to provide insight into the issues being discovered through accreditation efforts. EHNAC regularly works with the Office of the National Coordinator (ONC), the Office for Civil Rights (OCR), Veterans Administration (VA), and more, in an effort to share information and provide guidance as to best practices in protecting electronic healthcare information.

4. The role(s) of the government in enhancing cybersecurity for the private sector.

   EHNAC believes it is important for the government to provide feedback on best practices and support independent third party accreditation for organizations to enhance cybersecurity for vendors of healthcare software.

5. Performance measures for national-level cybersecurity policies; and related near-term and long-term goals.

   Measure compliance with OCR audits, EHNAC accreditations, and ONC certifications resulting in a report to highlight areas of highest frequency of weakness versus highest frequency of compliance so such policies may be adjusted in the weakest areas discovered. Goals may be established once a baseline compliance is determined.

6. Complexity of cybersecurity terminology and potential approaches to resolve, including common lexicons.

   Incorporate a glossary of terms or wiki that allows for updates from knowledgeable individuals with citations.

## 1. Current and Future Trends and Challenges

As technology has improved dramatically over the last decade, the public has often been left behind in understanding the cybersecurity risks and challenges. Moreover, they often do not hold users of their data accountable for breaches; and do not understand how to assure that their data is protected.

### 2. Progress being made to address the challenges

There has been some public notice of breaches which has raised public concern, but that concern is often short lived. The public tends to assume that security will be fixed without knowing how or even getting information about the fixes. Continued public awareness programs (like the HIPAA breach notification program) are helping with this.

### 3. The most promising approaches to addressing the challenges

Raising the awareness of the public to cybersecurity threats, challenges, and mitigation activities would be a promising avenue. Continued public pressure on organizations to protect cybersecurity would force further actions on mitigation.

### 4. What should be done now or within the next 1-2 years?

A public repository of identified breaches in all industries and actions organizations should take to prevent them would be helpful. A list of best practices, such as EHNAC has developed, should be made public so that all organizations can be held to those.

### 5. What should be done over the next decade?

Educational programs in high schools, colleges, and other public and private organizations need to be expanded so that the public can be better educated on cybersecurity and how to protect it.

Thank you for consideration of our comments and we look forward in any way we can assist to increase our efforts in the area of risk mitigation and assuring stakeholder trust.

Sincerely,

Lee B. Barrett

Lee Barrett, Executive Director

Cc: EHNAC Commission