Executive Summary – Health Care Industry Cybersecurity Task Force Report, June 2017

Key Takeaways:

- The state of cybersecurity in healthcare must improve and coordination across all industry stakeholders (federal agencies, Congress, healthcare providers, medical device manufacturers, accreditors, insurers, professional associations) is paramount.
- The federal government should provide additional resources and opportunities, starting with a new federal official to serve as a single point of contact to the industry on cybersecurity.
- Efforts must be undertaken to streamline and harmonize the federal requirements that may be in conflict or impeding enhanced cybersecurity hygiene.
- More can be done under current capabilities to enhance the security of medical devices and electronic health records (EHRs), but provider organizations must be able to manage and administer patches and improvements.

Background: On June 2, 2017, the Health Care Industry Cybersecurity Task Force released the "Report on Improving Cybersecurity in the Health Care Industry" to Congress fulfilling a statutory mandate from Section 405 of the Cybersecurity Act of 2015 included in the FY2015 Omnibus appropriations bill.

The Task Force, comprised of industry stakeholders referenced in the law (providers, payers, manufacturers, labs, security professionals, federal agencies, etc.) included CHIME Board members Theresa Meadows (Task Force co-chair) and David Finn, was given a year to meet and develop a report to be submitted to Congress no later than May 16, 2017.

Congress asked the Task Force to:

a. Analyze how other industries have implemented strategies and safeguards for addressing cybersecurity threats within their respective industries;
b. Analyze challenges and barriers private entities (excluding state and federal governments) in the healthcare industry face securing themselves against cyber attacks;
c. Review challenges that covered entities and business associates face in securing networked medical devices and other software or systems that connect to an EHR;
d. Provide the Department of Health and Human Services (HHS) with information to disseminate to healthcare industry stakeholders of all sizes for purposes of improving their preparedness for and response to cybersecurity threats affecting the industry;
e. Establish a plan for implementing cyber threat information sharing so that the federal government and healthcare industry stakeholders may in real time share actionable cyber threat indicators and defensive measures;
f. Report to appropriate Congressional Committees on the findings and recommendations of the task force.

Report Findings: The report portrays an industry in need of urgent action, as all entities within the sector remain a target for bad actors, with the significant potential to jeopardize patient care and safety. The Report breaks down the issue of healthcare cybersecurity into six imperatives, outlining a variety of topics within each imperative. Further the Report offers by top-level recommendations and action items for consideration by policymakers and other relevant stakeholders.

The imperatives identified in the report are:

1. Define and streamline leadership, governance, and expectations for health care industry cybersecurity;
2. Increase the security and resilience of medical devices and health IT;
3. Develop the health care workforce capacity necessary to prioritize and ensure cybersecurity awareness and technical capabilities;
4. Increase health care industry readiness through improved cybersecurity awareness and education.
5. Identify mechanisms to protect R&D efforts and intellectual property from attacks or exposure
6. Improve information sharing of industry threats, risks, and mitigations.

The action items have been broken down by the party tasked with executing them by the Task Force.

Action Items for CIOs and CISOs:

Action Item 2.1.1: Health delivery organizations must: 1) inventory their clinical environments and document unsupported operating systems, devices, and EHR systems; 2) replace or upgrade systems with supported alternatives that have superior security controls where possible; 3) develop and document retirement timelines where devices cannot yet be replaced; and 4) leverage segmentation, isolation, hardening, and other compensating risk reduction strategies for the remainder of their use.

Action Item 2.1.3: For devices that still receive some support from the device manufacturer and/or application vendor, these organizations must make real-time updates and patches (e.g., to the operating system), as well as make compensating controls available to end users. Organizations should also have a policy/plan in place to be able to receive and implement available updates.

Action Item 2.5.5: Health care providers should ensure collaboration among department leadership, biomedical engineering teams, IT staff, and IT security in the selection, deployment, and maintenance of medical devices.

Action Item 4.1.3: Health care organizations should participate in National Cybersecurity Awareness Month events in their area and become partners of the National Cybersecurity Awareness Campaign, managed through DHS as a baseline to build and customize for the HPH Sector.

Action Item 4.2.3: Health care organizations must develop a strategy for cybersecurity hygiene for existing and legacy equipment, a systematic approach for patching, implementation of compensating controls, isolation, and/or replacement (as available or applicable) should be applied. For newly produced equipment/software entering the market, device manufacturers should have a plan for providing validated software updates and patches as needed throughout the lifecycle of the medical device.

Action Item 5.2.4: Health care providers should exercise solid due diligence processes when selecting third party solutions or cloud-based solutions, as well as ensure that sufficient administrative safeguards are in place, including an unlimited indemnification clause in case of data breaches.

Action Item 5.2.2: Entities that manage big data solutions should have detailed documentation of source and destination connections and diligent review and approval process in managing these connections.

Action Item 5.2.3: Entities that manage big data solutions should apply minimum necessary security principles in providing users/organizations with access to these systems to mitigate disastrous situations with these systems.

Action Item 5.2.5: Entities that manage big data solutions should apply extreme care in determining what data is collected, what data is retained, and what data is deleted as more data presents increased security risks.

Actions Items for Professional Associations (CHIME & AEHIS):
Action Item 4.1.1: Trade and professional associations should ensure cyber workforce training and education focuses on corporate officers and Boards of Directors communication.

Action Item 4.1.2: Trade and professional associations in the health care industry should develop materials for CISOs and security leaders to better communicate with executive level leadership and Boards of Directors regarding security risks, priorities, and cyber hygiene posture.

Action Items for the "Industry":
Action Item 2.2.2: Industry should actively participate in information sharing programs to better recognize and manage cybersecurity vulnerabilities and threats.
Action Item 1.4.1: Industry should establish scalable best practices for governance of cybersecurity across the health care industry. Action Item 1.4.2: The health care industry should incorporate governance issues in the health care-specific Cybersecurity Framework discussed in Recommendation 1.2, and should commit to its adoption.

Action Item 2.3.5: Industry should develop processes for assessing risks for integrated systems that cross regulatory boundaries, such as EHRs and medical devices.

Action Item 2.3.6: Industry should develop recommendations for incorporating patient safety and clinical hazards into the Common Vulnerability Scoring System (CVSS) for better risk management.

Action Item 2.4.1: Until a national standard exists, health care stakeholders should work collaboratively to establish standards for device-device authentication such that interoperability is not impeded.

Action Item 2.4.2: In situations where the provider is accessing an EHR or Health Information Exchange external to the hospital or clinical environment, the health care industry should adopt the NIST SP 800-46 guidelines for remote access including the use of two-factor authentication to ensure a compromised password cannot alone be used to gain access.

Action Item 2.5.2: Industry should establish a task force to collaborate on issues related to risks and challenges of product interdependencies and two-way data flows. These interdependencies include medical devices, EHRs, Internet of Things (IoT), and two-way data flows.

Action Item 2.5.4: Industry should build and anticipate the need for IT forensics to accompany adverse event investigations by ensuring that logs exist and are accessible.

Action Item 3.1.1: Industry should establish best practices for the qualifications and governance models that support the cybersecurity and privacy leadership role within their organizations.

Action Item 3.1.2: Industry should establish governance structures to empower CISOs to express risks and advocate for resources with organizational leadership.

Action Item 3.1.3: Industry should identify opportunities for defining shared or third party CISO roles for small organizations.

Action Item 3.2.1: Industry should develop a research report, similar to the California Safe Patient Ratio, to identify appropriate voluntary benchmarks for cybersecurity staffing per patient accounting for various exceptions/factors (e.g., research centers/academic medical centers/ambulatory versus inpatient facilities).

Action Item 3.2.4: Industry should define mechanisms to educate and better leverage clinicians, in a tiered workforce model, capable of fundamental cybersecurity-related tasks.

Action Item 3.4.4: Industry should develop use cases and contracts tailored for these small and medium-size organizations.

Action Item 4.4.3: In order to establish an industry-wide baseline, the self-assessment should be required for all Covered Entities while granting exemption or partial exemption to fines or prosecution as a result of that assessment and corrective action plans.

Action Item 4.2.1: Industry should manage all health care infrastructure technology (including IoT) security to focus on patient safety, both on an individual and population basis, with an appreciation of how the technology will be used and how it could be misused.

Action Item 5.1.2: Industry should develop best practices to balance academic freedom, intellectual property, and health care services.

Action Item 6.1.2: Industry should incentivize the adoption of information sharing for small and medium-sized organizations for MSSPs.

Action Item 6.3.2: Industry should implement cybersecurity incident response plans, which are reviewed and tested annually.

Action Items for Medical Device Manufacturers:
Action Item 2.2.1: Manufacturers and developers must create a "bill of materials" that describes its components (e.g., equipment, software, open source, materials), as well as any known risks associated with those components to enable health care delivery organizations to more quickly determine if they are impacted.
Action Item 2.2.3: Industry (e.g., manufacturers, vulnerability finders, etc.) must adopt and engage in coordinated vulnerability disclosure consistent with recognized standards (e.g., ISO/IEC 29147and ISO/IEC 3011144).

Action Item 2.3.1: Manufacturers, developers, and users should implement security by design throughout the product lifecycle, including operations and maintenance.

Action Item 2.3.2: Manufacturers and developers should plan for operations and maintenance to ensure continuous monitoring, ongoing patching, and weakness remediation.

Action Item 2.3.3: Industry must include threat modeling as a clear part of their SDL including their system development lifecycle (SDLC). Industry should recognize, characterize, and manage weaknesses relative to common attack patterns and evolving threats, ideally during design and development of the technology or post hoc in the form of compensating controls within the broader system environment into which the technology would be integrated.

Action Item 2.3.4: Manufacturers should better leverage and attest to mature standards for secure product lifecycle including secure SDLC across design, development, manufacturing, service, support, and through end of life.

Action Item 2.3.7: Manufacturers should provide instructions for secure configuration of devices on networks, documentation on secure preparation for recycling and disposal of medical devices, and specific guidance regarding supporting infrastructure architecture (e.g., network segmentation requirements). Ideally these instructions would include how to scrub any personally identifiable information, PHI, or other site-specific sensitive data such as configuration files.

Action Item 2.5.1: Manufacturers should focus on architecturally supporting security interoperability for their products that validate, and leverage health care delivery organizations existing security controls.

Action Item 4.2.2: Industry should ensure that no known malware exists in newly produced equipment/software entering the market (i.e., premarket), and there should be ongoing surveillance for malware in equipment/software currently in the market (i.e., postmarket).

Action Items for Insurance Companies:
Action Item 3.4.5: Insurance companies should provide more incentives to encourage small and medium-size health care service providers who migrate to a more secure environment than the one in which they currently operate.

Action Items for Healthcare Accrediting Organizations:
Action Item 2.1.2: Health care sector accreditation organizations (e.g., Joint Commission, and Centers for Medicare & Medicaid Services (CMS) must: 1) consider incentives, requirements, and/or guidelines for reporting and/or use of unsupported system and mitigation strategies; and 2) develop aggressive timelines for conformance.

Action Items for Congress:
Action Item 1.5.1: Congress should explore potential impacts of the Physician Self-Referral Law and the Anti-Kickback Statute on collaborative industry cybersecurity efforts and identify potential modifications or exemptions as appropriate.

Action Item 1.5.2: Congress should establish a task force to make recommendations for harmonization of existing and future laws to remove the resource and financial burdens, such as those created by other fraud and abuse laws, and allow organizations to implement cybersecurity frameworks that will keep patients safe from cybersecurity threats.

Action Item 3.2.5: Congress should provide financial support to CNSS and CAE-CD for cybersecurity education certification to ensure core competencies for health care cybersecurity professionals.

Action Item 5.1.4: Congress should identify resources for improving research addressing small and rural provider security challenges.

Action Items for HHS:
Recommendation 1.1: Create a cybersecurity leader role within HHS to align industry-facing efforts for health care cybersecurity.

Action Item 1.1.2: The HHS Secretary must task the cybersecurity leader to work with federal, state, and industry partners to create a plan to establish goals and priorities for health care sector cybersecurity.

Action Item 1.1.3: The HHS Secretary must authorize the cybersecurity leader to define the reporting lines directly to other federal agencies tasked with cybersecurity such as the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and others.

Action Item 1.1.4: The cybersecurity leader must assist in streamlining HHS' outreach in a consistent manner to industry (e.g., branding, alignment with the NIST Cybersecurity Framework).

Action Item 1.1.5: The cybersecurity leader should establish a mechanism for partnering with and gathering industry input to prioritize short- and long-term goals, such as a federal advisory committee or similar mechanism.

Action Item 1.1.6: The cybersecurity leader should coordinate with U.S. and international intelligence agencies to ensure that Vulnerability Equities Process-like processes respect the special nature of digital health technology. Additionally, the cybersecurity leader should contribute to ongoing international policymaking and best practice development in this area.

Action Item 1.2.1: HHS should complete work on the Act Section 405 (d) for Aligning Health Care Industry Security Approaches through a consensus-based approach to develop a health care sector specific cybersecurity framework.

Action Item 1.2.2: HHS and NIST must develop guidance about how to apply the framework to the health care sector.

Action Item 1.3.1: HHS, in coordination with the private sector, federal, and state partners should look across HHS to harmonize regulations that directly or indirectly apply cybersecurity standards or best practices to reduce the burden on the industry.

Action Item 1.3.2: HHS should make recommendations to Congress about required statutory changes.

Action Item 1.3.3: HHS must publish standards and guidance consistent with the NIST Cybersecurity Framework. These should be developed based on the structure of the framework, as opposed to a mapping after the fact.

Action Item 1.3.4: HHS should establish a Task Force to explore options to incentivize risk-based cybersecurity in alignment with their existing oversight roles.

Action Item 1.3.5: HHS should develop a conformity assessment model37 built upon a public/private partnership to standardize cybersecurity compliance consistently across programs. Conformity assessments conducted by private sector organizations can increase productivity and efficiency and by encouraging federal agencies to standardize expectations.

Action Item 2.5.3: HHS should evaluate existing authorities and identify gaps to conduct cybersecurity surveillance of medical devices and EHRs.

Action Item 3.2.2: HHS should consider options, in coordination with industry partners, to develop a conformity assessment program to establish standards for different roles within the health care industry and authorize education providers against those standards.

Action Item 4.3.1: Health care regulatory agencies in partnership with industry should establish the requirements for a common set of requirements upon which the conformity assessment program would be built.

Action Item 4.3.3: Health care regulatory agencies should develop strategies to begin to phase in certifiers who have been accredited under the conformity assessment program.

Action Item 4.3.5: Health care regulatory agencies should be familiar and continue to build upon the National Cybersecurity Workforce Framework60 for an understanding of cybersecurity roles, responsibilities, and the knowledge, skills, and abilities required for each cybersecurity role. The Workforce Framework is available at Workforce Framework.

Action Item 4.5.1: HHS should work with government and industry partners to develop an outreach and engagement campaign to increase health care cybersecurity awareness and literacy among health care providers, patients, and IT professionals.

Action Item 4.5.2: HHS should work with government and industry partners to develop a specific outreach program for health care executives, so that they can have a better understanding of the importance of cybersecurity in their own organizations and can better engage with cybersecurity professionals to ensure that protective programs are adequately managed and resourced.

Action Item 4.5.3: HHS should work with government and industry partners to develop a series of workshops to explore current questions in health care cybersecurity, such as evaluation of best practices, research and development (R&D) needs, and the role of insurance.

Action Item 4.5.4: HHS should work with government and industry partners to develop educational materials for patients to assist them in accessing, managing, and protecting their health care information.

Action Item 4.5.5: HHS should work with government and industry partners to develop a national health care cyber-literacy course that is updated on a biannual basis to keep up with rapidly changing technology and to train health care professionals on the importance of cybersecurity in their day-to-day tasks. Industry at all levels should incorporate principles from this course into all patient education modules or courses, as applicable.

Action Item 4.5.6: HHS should work with government and industry partners to develop a health care mentoring program to help educate non-IT staff to proper risk management of IT and information sharing.

Action Item 4.5.7: HHS should identify privacy experts, patient advocates, regulatory experts, and proprietary information experts to discuss issues related to fraud or stock manipulation.

Action Item 5.1.5: HHS should partner with DHS and Office of the Director of National Intelligence to identify specific threat actors and the techniques that they employ to target U.S. health care R&D

information. This information should be updated regularly to stay abreast of emerging tactics and techniques.

Action Item 5.1.6: HHS should present findings from Action Item 5.1.5 to senior executives and other representatives from the R&D industry.

Action Item 5.1.3: HHS should partner with the DHS Science and Technology Directorate to identify grand challenges, priorities, and implement new research to support small and rural organizations.

Action Item 6.1.1: HHS in cooperation with the ISAOs should streamline and consolidate information sharing data on threats whenever practical for easier consumer adoption.

Action Item 6.2.1: HHS in coordination with ISAOs should evaluate incorporating hazards (e.g., national disasters, acts of terrorism, pandemic outbreaks) with the potential to disrupt critical health infrastructure in their information sharing threat analysis.

Action Item 6.2.2: HHS should work with all federal partners to ensure that intelligence reports and threat information is consolidated and given additional context as distributed to industry.

Action Item 6.2.4: HHS and the ISAO should continue to work with DHS and other entities to develop processes for quickly curating and releasing critical threat information.

Joint Action Items for Government and Industry:
Action Item 2.1.4: Government and industry should develop incentive recommendations to phase-out legacy and insecure health care technologies (e.g., incentive models like Cash for Clunkers, Montreal Protocol, and Federal IT Modernization Fund). As a part of looking at incentives, government and industry should create partnerships/alliances to establish roadmaps for joint enhancement of cybersecurity interoperability and maturity through better procurement processes.

Action Item 1.2.3: Industry and government should partner to establish an evaluation mechanism and prioritized best practices to support the range of small to large organizations to consistently apply the NIST Cybersecurity Framework.

Action Item 2.3.8: Industry and government should consider issuing a grand challenge, soliciting from stakeholders novel incentive structures that could be leveraged to address cybersecurity challenges specific to securing legacy systems, SDL, strategic and architectural approaches, and holistic data flow and system requirements for EHRs (e.g., creating a challenge which develops or identifies reference architectures and operating systems for safety critical systems which are higher assurance, more interoperable, and supported for longer periods of time).

Action Item 2.6.1: Federal agencies must partner with industry to define the scope and scale of a MedCERT. The MedCERT would be a trusted entity that is viewed as independent and neutral by all stakeholders and will work to arrive at “the ground truth” of vulnerabilities and proposed mitigations.

Action Item 2.6.2: In order to validate the vulnerabilities and impacts, as well as assess the public fixes (mitigations and patches), the MedCERT will need to rely upon the technical analyses provided by

independent certification and testing capabilities. These technical analyses provided by individual testing labs will need to be correlated to support the MedCERT's vulnerability validation and assessment roles.

Action Item 3.2.6: Industry and the federal government should explore opportunities for individuals to engage in ongoing internship programs to develop more information security professionals in supporting the health care industry.

Action Item 3.3.3: Industry and the federal government should explore opportunities for individuals to engage in ongoing internship programs (e.g., at MSSPs and federal agencies) to develop more information security professionals in supporting the health care industry.

Action Item 6.3.1: HHS and industry should identify those critical incident response plans that could be best leveraged by the health care industry.

Action Item 4.3.4: The federal government in coordination with industry should develop a business model/incentives to ensure that the testing, validation, and certification data is widely available to health care providers, regardless of size and resources.

Action Item 6.2.3: HHS should partner with industry to identify health care subsector priorities for intelligence reporting. For example, payers may be extremely interested in information regarding medical insurance fraud and emerging cybercrime tactics that are used to support this activity, whereas pharmaceutical companies are likely to be very interested in the changing methods used by nation state actors to steal intellectual property.

Action Item 5.1.1: The federal government should work with industry to establish a task force to develop risk models for evaluating U.S. economic and organizational impact for cybersecurity failures.

Action Items for Other Federal Government Agencies or Agency Collaboration:
Action Item 2.3.9: Government agencies (e.g., FDA and HHS Office of the National Coordinator for Health Information Technology) should consider how they can use their existing authorities to catalyze and reinforce activities and action items associated with this recommendation. Areas of interest may include unsupported operating systems, hardcoded passwords, tactical guidance related to evolving threats like botnets or ransomware, etc.

Action Item 3.2.3: Organizations such as the Committee on National Security Systems (CNSS), the National Centers of Academic Excellence in Cyber Defense (CAE-CD), DHS, or NIST should consider establishing mechanisms to assist in developing the requirements for and certifying advanced degree cybersecurity programs.

Action Item 3.3.1: The federal government should evaluate incentive options, such as grants and tax incentives, to encourage more MSSPs to achieve economies of scale to support small and medium-size health care providers.

Action Item 3.3.2: Federal regulatory agencies should evaluate incentive options, such as crediting small and medium-size health care providers who have engaged MSSPs during their audits and breach investigations, to encourage providers to leverage MSSPs.

Action Item 3.4.1: The federal government should evaluate incentive options, such as grants, to encourage industry to develop secure options for supporting small and medium-size health care organizations.

Action Item 3.4.2: The federal government should evaluate incentive options, such as tax incentives, to encourage health care providers migrate to more secure environments including hosted services (i.e., vendors or other providers) or cloud service providers.

Action Item 3.4.3: Federal regulatory agencies should provide additional guidance to service providers (including HHS-compliant Business Associate Agreements) that wish to align their security management practices with HIPAA and create increased awareness among health care providers that alternative technologies exist to store, access, share, and process their data.

Action Item 4.4.1: HHS and NIST should develop a health care specific version of the NIST Baldridge Cybersecurity Excellence Builder.

Action Item 4.4.2: HHS and NIST should develop a tiered version of the tool for the industry based on size and business model (e.g., physician practice, clinic, hospital, Academic Medical Center, business associates).

Action Item 4.3.2: The federal government should resource and establish a process for the oversight of the conformity assessment program.

Action Item 4.6.1: The FTC should engage health care and consumer organizations to develop a process to evaluate, assess, and rate health care/lifestyle products. This aligns to action item 3.1.3 of the Commission on Enhancing National Cybersecurity's Report on Securing and Growing the Digital Economy.

Action Item 4.6.2: HHS, DHS, NIST, and FTC should establish a grant or national challenge for a consumer grading system.

Action Item 6.3.3: HHS, DHS National Cybersecurity and Communications Integration Center (NCIC), and law enforcement should maintain unified and dedicated channels during steady state and response efforts to: 1) provide subject matter expertise to issues that involve the HPH Sector; 2) leverage existing sector relationships across government, within industry, and with an impacted entity; and 3) facilitate targeted dissemination, clarification, and near real-time notifications to the health care industry in a strategically sequenced manner.

Action Item 6.4.1: HHS, DHS, and the FBI should review the HPH Sector's utilization of the Private Sector Clearance Program to identify gaps and strengthen the criteria and process through which health care industry partners can apply for clearances.