S. HRG. 117–398

CYBERSECURITY IN THE HEALTH AND EDUCATION SECTORS

HEARING

OF THE

COMMITTEE ON HEALTH, EDUCATION, LABOR, AND PENSIONS

UNITED STATES SENATE

ONE HUNDRED SEVENTEENTH CONGRESS

SECOND SESSION

ON

EXAMINING CYBERSECURITY IN THE HEALTH AND EDUCATION SECTORS

MAY 18, 2022

Printed for the use of the Committee on Health, Education, Labor, and Pensions

Available via the World Wide Web: *http://www.govinfo.gov*

U.S. GOVERNMENT PUBLISHING OFFICE

48–909 PDF WASHINGTON : 2024

COMMITTEE ON HEALTH, EDUCATION, LABOR, AND PENSIONS

PATTY MURRAY, Washington, *Chair*

BERNIE SANDERS (I), Vermont
ROBERT P. CASEY, JR., Pennsylvania
TAMMY BALDWIN, Wisconsin
CHRISTOPHER S. MURPHY, Connecticut
TIM KAINE, Virginia
MAGGIE HASSAN, New Hampshire
TINA SMITH, Minnesota
JACKY ROSEN, Nevada
BEN RAY LUJAN, New Mexico
JOHN HICKENLOOPER, Colorado

RICHARD BURR, North Carolina, *Ranking Member*
RAND PAUL, M.D., Kentucky
SUSAN M. COLLINS, Maine
BILL CASSIDY, M.D., Louisiana
LISA MURKOWSKI, Alaska
MIKE BRAUN, Indiana
ROGER MARSHALL, M.D., Kansas
TIM SCOTT, South Carolina
MITT ROMNEY, Utah
TOMMY TUBERVILLE, Alabama
JERRY MORAN, Kansas

EVAN T. SCHATZ, *Staff Director*
DAVID P. CLEARY, *Republican Staff Director*
JOHN RIGHTER, *Deputy Staff Director*

C O N T E N T S

STATEMENTS

WEDNESDAY, MAY 18, 2022

CYBERSECURITY IN THE HEALTH AND EDUCATION SECTORS

Wednesday, May 18, 2022

U.S. SENATE,
COMMITTEE ON HEALTH, EDUCATION, LABOR, AND PENSIONS,
Washington, DC.

The Committee met, pursuant to notice, at 10:01 a.m., in room 216, Hart Senate Office Building, Hon. Patty Murray, Chair of the Committee, presiding.

Present: Senators Murray [presiding], Casey, Baldwin, Murphy, Hassan, Hickenlooper, Cassidy, Braun, Scott, and Tuberville.

OPENING STATEMENT OF SENATOR MURRAY

The CHAIR. Good morning. The Senate Health, Education, Labor, and Pensions Committee will please come to order. Today we are having a hearing on cybersecurity in the health and education sectors. I will have an opening statement followed by Senator Cassidy, and then we will introduce our witnesses. After they give their testimony, Senators will each have 5 minutes for a round of questions.

Again, while we were unable to have this hearing fully open to the public or media for in-person attendance, live video is available on our Committee website at *help.senate.gov*. And again, if you are in need of accommodations including closed captioning, please reach out to the Committee or the Office of Congressional Accessibility Services.

Every day, students, educators, patients, and health care providers across the country rely on countless programs and IT systems to learn with online tools, to get a prescription, do a telehealth appointment, and so much more.

It is easy to take for granted how critical technology is to fundamental tasks like collecting and protecting the personal data of students and patients. Keeping track of course requirements, lesson plans, student financial aid, or providing information about prescriptions, allergies, and surgeries, information with potentially life and death consequences.

During the past few years, COVID–19 has made technology even more central in health care and education, as patients and providers have made greater use of telehealth services to make care accessible and schools are helping close the digital divide by connecting students to the internet and devices.

With that increased reliance on technology, we must also increase the attention given to the challenges that technology

present. A critical part of that is closing the digital divide and ensuring all of our communities have access to the internet, which is why I fought so hard to invest in universal broadband and digital equity in our bipartisan infrastructure law. But we can't just call it a day after we make technology easy to use or access. We need to make sure it is also safe and secure.

We need to address cybersecurity attacks and ensure they are treated like the National Security threat they are because cyber-attacks are on the rise. In 2020, 70 percent of hospitals surveyed said they had faced a significant security incident within the past 12 months. And between 2016 and 2021, there were over 1,300 school cybersecurity incidents in the U.S. and that is just counting the ones that were publicly disclosed.

In my home State of Washington, we know that there were at least 44 data breaches in the health care sector last year and at least 35 in education. And the number of cyber-attacks in our state overall increased significantly from 2020, with the number of large scale attacks affecting over 50,000 people having tripled.

During this pandemic, we also saw hackers infiltrate our state's unemployment insurance system, a breach that exposed the information of over a million people across my state. These attacks can come from a wide variety of sources, individual hackers, organized crime, and even hostile state actors, as we have seen most recently in Russia's invasion of Ukraine.

This is a serious National Security threat and families need to know we are taking action to keep them safe from our enemies here. Because we know our biggest global adversaries, Russia, China, North Korea, Iran have been putting resources into sharpening their cyber-attack capacity.

Cyber-attacks can also take a wide variety of forms. Data breaches that expose sensitive information from health information adversaries might use to threaten National Security to private financial information about patients, students, and staff, distributed denial of service attacks that can be used by hostile countries and others to make computers and networks unresponsive and shut down services, or ransomware attacks where foreign actors or other dangerous organizations hold essential services and data hostage unless a large financial ransom is paid.

Even when a hospital or school is doing everything right, there are always new threats they may not be able to be prepared for. And every organization is still vulnerable to attacks on the tech vendors that they rely on. For example, a 2019 cyber-attack on Pearson affected over 13,000 students and a breach at another education vendor last year, Blackbaud, exposed the financial information of 17,000 students just from my home State of Washington alone.

The fallout from these attacks can be devastating and wide ranging. Hospitals can get locked out of the electronic health care records they need to understand a patient's condition or software needed to schedule surgeries or track prescriptions or get lab results and divert ambulances. I have even heard from health departments back in Washington State about how responding to cyber-attacks has pulled resources and staff from their COVID vaccination

efforts. These kinds of challenges don't just cause major headaches or losses and expenses, they put patients in danger, they undermine our National Security, and in some cases, they even cost lives.

Meanwhile, our schools are at risk of getting locked out of online programs that students use to get in turn in assignments or teachers used to post and track grades, and administrators use to layout courses and schedules for the semester. Hacks can disrupt routine and functions like payroll, and can leave patients, students, and staff exposed to identity theft. And that can be especially concerning for K–12 students, as it often isn't clear to students or parents that a child's identity has been stolen until they try to open a bank account or request student aid, which may not happen for several years.

Cyber-attacks also have huge implications for our Country as a whole. They can undermine our competitiveness on the world stage. And the possibility of a cyber-attack coordinated by our enemies to take out health care facilities, especially at a moment of crisis, is a serious threat. So we have to make sure we are ready and vigilant.

That is why I am glad President Biden signed into law legislation we passed to require more reporting of cyber incidents and to study the impact of cyber-attacks on K–12 schools. It is why I am now watching closely as HHS works to strengthen its information security systems and as ED works to help protect K–12 schools from cyber-attacks, and it is why today's hearing is so important.

I want to hear from all of our witnesses about how we can address urgent challenges, like how do we recruit, train, and retain more cybersecurity experts, especially in the health and education sectors where there is a big shortage? What are some best practices that schools and health care providers should be implementing? And how can we better connect organizations to share information like this that will help prevent, mitigate, and respond to cybersecurity incidents? How can we improve disclosure of cybersecurity incidents so people will know when and how they have been affected by a hack, what they might do about it, and how can they protect themselves? And what are we doing to prepare for attacks from hostile foreign actors? How do we make sure we don't just keep up but keep ahead of Russia, China, North Korea, Iran, and others?

It is especially critical to me that we are treating cyber-attacks like the National Security threat we know they are. These are incredibly important questions for families back at home in Washington State and across the entire country whose privacy, finances, futures, and even lives depend on making sure we have good answers and take clear steps to put them in practice.

I look forward to hearing from all of our witnesses today about these issues and really appreciate all of you being here. With that, I will turn it over to Senator Cassidy for his opening remarks.

OPENING STATEMENT OF SENATOR CASSIDY

Senator CASSIDY. Thank you, Madam Chair. Good morning. Thank you all for attending today's hearing on cybersecurity in the

health and education sectors. Looking at you out there, I feel like I am Vladimir Putin meeting with his generals, like on a table 60 yards long. But thank you for being here. In April 2020, the FBI announced that it expected cyber-attacks to increase as a result of a shift to virtual environments during the pandemic. Their prediction was correct.

While cyber threats impact nearly every aspect of our daily lives, we are discussing just two. According to data from the K through 12 Cyber Security Resource Center, K–12 schools have experienced an 18 percent increase in cyber-attacks in 2020 compared to 2019. Specifically, 317 school districts across 40 states suffered 408 publicly disclosed cyber security incidences in 2020.

Microsoft Security Intelligence found that 61 percent of nearly 7.7 million enterprise malware encounters reported in May 2020 came from the education sector, making it the most affected industry. With regard to health care, nearly 50 million people in the U.S. had their sensitive health data breached in 2021, more than triple 2018 numbers.

Just last month, U.S. Federal agencies led by the Cybersecurity and Infrastructure Security Agency issued the strongest warning yet of cyber-attacks on critical infrastructure by Russian government security and intelligence services retaliating against any organization providing support to Ukraine. So what exactly are these cyber threats and incidences in both health and education, the industries being hit by ransomware and phishing attacks? In the health industry, patient care is time sensitive.

As a doctor, I cannot express enough the importance of timeliness in care. Cyber-attacks to delay care cost American lives, and that was particularly during the pandemic. A September 2021 CISA report found that ransomware cyber-attacks on hospitals led to significant and sustained hospital strain and related consequences such as IT network failure, ambulance diversion, strain on ICU bed utilization, and increased mortality.

We must talk today about stopping adversaries from denying our patients the care that is needed. Cyber-attacks are never a victimless crime. In K through 12, phishing attacks stealing data from our youngest children are especially concerning because it can take years to discover that a child's identity has been stolen. In the meantime, the thieves can open credit cards and mount up large debts with a child's identifying information.

Ransomware attacks, on the other hand, show themselves immediately and can result in significant disruptions in the classroom. These attacks come at a high cost, both in the ransom paid and the work it takes to restore systems. One higher education example, University of California San Francisco Medical School paid $1.14 million to hackers who encrypted and threatened to publish sensitive information stolen from the institution.

In another health care example, universal health care services, or UHC, experienced a cyber-attack in October 2020, costing UHC $67 million in lost revenue and recovery efforts. Collaboration with and among the private sector is essential to solving this problem. Existing partnerships with organizations like some of the ones you represent, as well as closer collaboration among Federal agencies,

are key ingredients we must pursue as a long term solution to cyber vulnerability.

A strong cyber defense to protect our Country from virtual threats is becoming just as important as a strong military and police force to defend from physical threats. From the bipartisan infrastructure bill to military aid for Ukraine, nearly every comprehensive piece of legislation has to consider and address the importance of cybersecurity.

Continuing that discussion in regards to Americans health and education is also needed. It is important that the Committee is doing this today. With that, I look forward to hearing from our witnesses about how to improve cybersecurity protocols on the Federal level. And I yield.

The CHAIR. Thank you, Senator Cassidy. I will now introduce today's witnesses. Our first witness is Denise Anderson, President and CEO of the Health Information Sharing and Analysis Center, or ISAC a nonprofit organization dedicated to protecting the health sector from physical and cyber-attacks and incidents by serving as a trusted and timely resource for information.

Ms. Anderson is also Chair of the National Council of ISACs, on the Board of Directors for the Global Resilience Federation, on the Cyber Working Group Executive Committee for the Health and Public Health Sector Coordinating Council and engaged in a number of other groups and initiatives focused on cyber issues in the health care sector.

Ms. Anderson, thank you for joining us today. I look forward to your testimony. And with that, I am going to turn over to Senator Hassan, who will introduce our next witness, Joshua Corman.

Senator HASSAN. Well, thank you so much, Chair Murray. It is a real pleasure to introduce our second witness today, Mr. Joshua Corman from Dover, New Hampshire. He is joined today by his fiance, Andra. Thank you for being here as well. Mr. Corman is a founder of a volunteer organization called I Am the Cavalry, which focuses on using the cybersecurity skills of its members to protect public safety.

He also recently served as the Chief Strategist on the Cybersecurity and Infrastructure Security Agency, or CISA's COVID Task Force, where he worked to protect the healthcare sector from cyberattacks and cyber espionage, as the COVID–19 pandemic strained the sector.

He has previously served in several different senior cybersecurity and technology roles, including as Chief Security Officer at PTC, a software company, Director of the Cyber Statecraft Initiative for the Atlantic Council, and Chief Technology Officer for Sonatype, a cybersecurity company. He also serves as an adjunct faculty for the Chief Information Security Officer Certificate Program at Carnegie Mellon University.

As someone who has worked with Members of both parties to strengthen cybersecurity at all levels of Government, especially in small communities, I appreciate Mr. Corman's work very much. Welcome, and thank you for your service, Mr. Corman. I look forward to your testimony today.

The CHAIR. Thank you, Senator Hassan. Today, we will also be hearing from Amy McLaughlin, a knowledgeable technology and information security leader with experience in education, finance, medical, and Government sectors. Ms. McLaughlin is the Cybersecurity Program Director at the Consortium of School Networking.

That is an organization focused on meeting the technology needs of K–12 leaders and supporting the entire IT system, team and school systems. She is also the Executive Director of Technology and Solutions Architecture at Oregon State University. Thank you for joining us today. We look forward to your testimony.

Finally, our last witness today is Helen Norris. She is Vice President and Chief Information Officer at Chapman University. She is responsible for leading the university's information technology strategy and services and overseeing the university library.

She is also a Board Chair of EDUCAUSE, a nonprofit whose mission is to advance higher education through the use of information technology. We look forward to hearing from you today as well. And thank you again to all of you for joining us today. With that, we will begin testimony. Ms. Anderson, we will start with you.

STATEMENT OF DENISE ANDERSON, PRESIDENT AND CEO, HEALTH INFORMATION SHARING AND ANALYSIS CENTER, OAKTON, VA

Ms. ANDERSON. Good morning, Chair Murray, and Members of the Committee. My name is Denise Anderson, as you mentioned, and I am President and CEO of the Health ISAC. I am also representing the Health Sector Coordinating Council Cybersecurity Working Group. I want to thank you for the opportunity to speak today. Health ISAC is a global nonprofit. Our members range from small to large organizations and represent approximately two-thirds of the U.S. health and public health GDP.

Members include providers, academic medical centers, and medical device and pharmaceutical manufacturers, among others. Recently, Health ISAC published its report on the current and emerging health care cyberthreat landscape. And last month, Health ISAC worked with Microsoft to take down a Zloader malware family through coordinated legal and technical actions.

The takedowns struck a major blow against cybercriminals using ransomware to extort hospitals and other victims. The Health Sector Coordinating Council Cybersecurity Working Group is a volunteer coalition of 320 organizations. Membership is open to any organization that meet certain criteria. It is organized into task groups that work to develop best practices for various health care cybersecurity disciplines.

The CWG has produced 15 best practices publications which are freely available via their public website. Both Health ISAC and the CWG worked closely with HHS and the FDA as well as CISA. Our ongoing engagement includes weekly calls with the leadership in each organization to assess and discuss issues facing the sector. With the rise in digital health care, the proliferation of advances in technology, and the efficiencies of connecting devices and data, the cyber threat surface in health care has ballooned and the threat actors have followed.

The focus has traditionally been on data and privacy, but if providers cannot deliver services or data is manipulated or destroyed, patient lives can be at risk. Ransomware has had a big impact on the health sector. According to the FBI's 2021 Internet Crime Report, the sector experienced at least 148 ransomware attacks between June and December 2021, resulting in millions of dollars of losses.

Conti and its Ryuk Ransomware have been especially prolific. Ryuk has been linked to more than 200 ransomware attacks impacting health facilities, with revenue losses amounting to nearly $100 million and remediation costs of $500 million. A high profile attack as a result of Conti was against the national health system in Ireland in May 2021. The attack brought down all of their IT systems and resulted in canceled surgeries and delayed medical care. It took 4 months to recover from that incident.

The other impact of ransomware is the downstream effects when suppliers are attacked. When a human resources firm was attacked in December 2021, hospitals were forced to manage payroll and staff scheduling manually during a surge in COVID–19 infections. In January 2021, a manufacturer essential in providing packaging for COVID–19 treatments was attacked and pharmaceutical manufacturers experienced slowdowns in package production and shipping during a vital period in the pandemic.

The COVID–19 pandemic spurred several incidents. Threat actors accessed sensitive documents for a COVID–19 vaccine at the European Medicines Agency, where the documents were stored. Actors attacked and blocked access to an Italian COVID–19 vaccination booking system, and organizations offering cold storage and delivery processes for keeping vaccines at safe temperatures were targeted.

A concerning threat actor trend has been the intention and ability to target the IT supply chain, such as the SolarWinds attack, to gain access to a larger group of victims. Vulnerabilities also posed a huge problem for the sector. This reported vulnerabilities increased for a fifth straight year. Over 18,000 were reported in 2021, and almost 20 percent of those were considered high risk.

With the tensions between Russia and Ukraine high, many fear a fall out like what occurred during the 2017 Petya attacks that impacted over 300 companies and cost over $10 billion. In February, Russian actors attacked Viasat, 1 hour before Russia invaded Ukraine. Internet users and wind turbines producing electricity in Europe were impacted. Even if health care is not directly targeted, cascading impacts such as access to communications and electricity can be substantial.

The health sector is highly interconnected. Sensitive patient information must move between entities to facilitate proper patient care and history. Hospitals use tens of thousands of medical devices, expensive devices are not easily replaced, and run on software that is no longer patched or supported.

In addition, many of these devices run 24 hours a day, 7 days a week, 365 days a year, so taking them offline or patching them is not—is complicated. As can be seen by the contributions of the

CWG and Health ISAC, industry dedicates endless hours to help ensure the sector is strong and secure.

The publications, webinars, workshops, exercises, the many alerts are free and open to the sector. The Zloader takedown will benefit countless organizations inside and outside of healthcare, and we look to do more of the same. Despite the number of great initiatives and efforts underway, we can no longer look at the challenges through just a cyber and or physical lens but must consider all threats to operational resilience.

As evidenced by Hurricane Maria in Puerto Rico and the impact on IV bag supply, ransomware attacks which have crippled the health care delivery, and the COVID–19 shut down in China affecting the supply of contrast fluid used in imaging, health organizations must constantly be focused on all threats to health care delivery and patient safety.

The health sector should be supported and incentivized in this vital effort. This concludes my testimony. Thank you again for the opportunity and look forward to your questions.

[The prepared statement of Ms. Anderson follows:]

PREPARED STATEMENT OF DENISE ANDERSON

ISAC Background

Chair Murray, Ranking Member Burr, and Members of the Committee, my name is Denise Anderson. I am President and CEO of the Health Information Sharing & Analysis Center (Health-ISAC), Chair of the National Council of ISACs (NCI) and serve on the Executive Committee of the Health Sector Coordinating Council Cybersecurity Working Group (HSCC CWG). I want to thank you for this opportunity to address the Committee on Health, Education, Labor, and Pensions about the industry perspective on cybersecurity threats to the Health sector and the resulting challenges and impacts, as well as the activities the sector is undertaking to combat these threats including collaborating and coordinating within, between and across the public and private critical infrastructure sectors.

ISACs were formed in response to the 1998 Presidential Decision Directive 63 (PDD 63), which called for the public and private sectors to work together to address cyber threats to the Nation's critical infrastructures. After 9/11, in response to Homeland Security Presidential Directive 7 (its 2013 successor, Presidential Policy Directive 21) and the Homeland Security Act, ISACs expanded their role to encompass physical threats to their respective sectors. Many ISACs have been in existence over a decade and in some cases over two decades.

ISACs are industry driven, trusted communities that promote the sharing of timely, actionable, and reliable information for their respective critical infrastructure sectors and provide forums for owner and operator sharing around threats, incidents, vulnerabilities, best practices, and mitigation strategies. ISACs are operational in nature and have strong reach into their sectors to gather and disseminate information quickly and efficiently. ISACs have been thriving and growing in recent years as owners and operators have seen the benefit to participating in these trusted communities, which is a testament to the value ISACs deliver to their members. ISACs coordinate with each other through the National Council of ISACs (NCI), a voluntary organization formed in 2003.

Health-ISAC Background

Health-ISAC, (*www.h-isac.org*) founded in 2010, is a 501(c)6 nonprofit organization and is funded primarily by its member firms through member dues. Since 2010 the membership has expanded to over 700 organizations including healthcare delivery organizations (HDOs), providers, academic medical centers, medical research and development centers, medical materials manufacturers and distributors, pharmaceutical and medical device manufacturers, retail pharmacies, laboratories and radiological centers, telehealth providers, electronic health record providers and pay-

ers representing approximately two-thirds of the US Health and Public Health GDP[1].

Health-ISAC members represent 79 percent of the top 103 hospital chains in the United States, 61 percent of the top 51 global medical device manufacturers, 84 percent of the top 25 global pharmaceutical manufacturers, 93 percent of Fortune 500 healthcare companies in the United States and 86 percent of electronic health record providers in the United States. Our members range from small organizations with less than one million dollars in annual revenue to large Fortune 50 organizations with over 238 billion dollars in annual revenue.

Health-ISAC is a global organization that has members headquartered in over 20 countries and membership is growing rapidly. Health-ISAC saw its largest member growth ever in 2021.

The mission of Health-ISAC is to empower trusted relationships in the global healthcare industry to prevent, detect and respond to cyber-and physical security events so that members can focus on improving health and saving lives.

Besides offering a trusted forum and community for sharing information around threats, vulnerabilities, best practices and mitigation strategies, Health-ISAC offers a number of other services such as global workshops and webinars, four annual summits—two in the United States, one in Europe and one in Asia, daily cyber and physical reports, alerts, targeted threat alerts, a monthly newsletter, a weekly blog on cybersecurity issues in healthcare, white papers, monthly member-only threat briefings, monthly podcasts, exercises, special interest groups, a number of working groups and committees and various technical tools and partner programs for members to use in their environments. In addition, the Health-ISAC Threat Intelligence Committee (TIC) sets the sector cyber threat level monthly, or as needed, and provides valuable insight and mitigation strategies when threats arise, or incidents occur.

Health-ISAC has numerous sharing and collaboration channels, including platforms where hundreds of thousands of actionable indicators and threat actor tactics, techniques, and procedures (TTPs) are shared. Health-ISAC was one of the first organizations to adopt STIX and TAXII, which are protocols for automated indicator and intelligence sharing and fosters a robust member machine-to-machine sharing environment. Health-ISAC uses the Traffic Light Protocol, (TLP) an information owner dissemination determination protocol for sharing of information. TLP RED is the most restricted sharing protocol, with TLP WHITE, the broadest. Over 100,000 individuals have access to our TLP GREEN and TLP WHITE alerts.

In 2021, for example, Health-ISAC:

- Provided alerts, papers, webinars, thought leadership and facilitated collaboration on myriad incidents during the year including SolarWinds, Accelion, ProxyLogon, PrintNightmare, VPN Vulnerabilities, in Fortinet, Pulse and Citrix, Colonial Pipeline, JBS Meats, Irish National Health Service, Kaseya, Geopolitical Tensions, Hurricane Ida and other physical threats, and Log4j.
- Added 119 new members amounting to a member community of over 5,500 individuals.
- Nearly tripled the number of member organizations using automated indicator sharing.
- Conducted 12 highly attended *Monthly Member Threat Briefings*, published 242 *Finished Intelligence Reports*, sent over 419 *Targeted Alerts*, held ten *Threat Operations Center (TOC) Spotlight* threat and vulnerability webinars, and distributed over 65,812 actionable indicators of compromise.
- Worked with security researchers to develop four pre-public alerts and vulnerability notifications impacting millions of medical devices.
- Stood up several new programs including a new webinar program, *Continue the Conversation* for members to bring subject matter expert panels and discussions around hot topics from the chat channels, the Microsoft Patch Tuesday Podcast and TOC Open House Office Hours.
- Hosted an Analytics Training Workshop, offered 63 webinars, and held three successful global in-person Summits, with our Fall Summit attendance close to pre-pandemic numbers. Health-ISAC also conducted nine

[1] Based on the annual revenue of all Health-ISAC member organizations. ($2.3 Trillion).

customized exercises and in 2022 published an After-Action report from our 2021 *Rethinking Resiliency* exercise series.

- Planned, and held the Hobby Exercise, a tabletop exercise designed to engage the Health sector and strategic partners, including those in government, on significant security and resilience challenges. The overarching objective is to inform and provide opportunities for continuous organizational improvement while increasing Health sector resiliency. The annual exercise is named for Oveta Culp Hobby, the first U.S. Secretary of Health, Education and Welfare. The 2021 After-Action Report illustrating findings from the exercise was recently published in March 2022.
- Worked with Cisco to conduct a well-received 2-day Leadership Development Course for rising CISOs at the 2021 Fall Summit. This was also held at our Spring Summit in May 2022.
- Produced four white papers, developed Pharmaceutical and Supply Chain Guidance for practitioners and healthcare CISOs, and expanded physical threat information deliverables for Health sector organizations. Also published *Full* and *Lite* versions of copyrighted *Health-ISAC Questionnaires* for Third-Party Risk Management. In 2022 we also published a white paper on *Securing the Modern Pharmaceutical Supply Chain*.
- Offered valuable tools for members such as third-party risk management, digital risk protection and internet traffic visualization through our Community Services Program.
- Facilitated five Committees, over 15 Working Groups and three Councils devoted to topics such as Cybersecurity Analytics, Information Security Incident Response, Security Engineering and Architecture, Business Resiliency and Cybersecurity Awareness and Training.
- Continued to build on our work to improve security across the Medical Device Community with over 25 medical device public advisories, two Food and Drug Administration (FDA) Town Halls at Health-ISAC Summits and curated medical device information related to Log4j and other vulnerabilities on the Health-ISAC website. Our Medical Device Cybersecurity Information Sharing Council is comprised of 331 individuals from 135 organizations with half of the group comprised of Healthcare Delivery Organizations (HDOs) and the other half comprised of Medical Device Manufacturers (MDMs).
- Conducted over 30-member interest surveys on topics such as SolarWinds Impact, Security Workforce Size and Strategy, and Security Operations Centers Resourcing.

In 2022, to date, Health-ISAC has engaged in five major activities of note. The first is the publishing of the first annual Health-ISAC report on the *Current and Emerging Healthcare Cyber Threat Landscape* in both TLP GREEN and TLP WHITE versions. The report features survey results on member threat perspectives, as well as, top issues from 2021 and a look ahead into 2022 (*https://h-isac.org/health-isacs-first-annual-current-and-emerging-healthcare-cyber-threat-landscape-executive-summary/*). The second is the publishing of the 2021 Health-ISAC Annual Report (*https://h-isac.org/2021-annual-report/*). Third, the ISAC held several webinars, produced alerts and briefings, and published a joint bulletin with the Health Sector Cybersecurity Coordination Center (HC3), part of the Department of Health and Human Services (HHS), regarding the geopolitical tensions in Russia. The ISAC emphasized several messages to the sector that resulted from Classified briefings conducted by the White House, Cybersecurity and Infrastructure Security Agency (CISA), and its partners and stood up a working group of members directly impacted by the situation so that they could share challenges, issues, and best practices with each other. Fourth, Health-ISAC worked on another pre-public vulnerability disclosure with CISA and CyberMDX/Forescout on Access: 7 vulnerabilities found in PTC Axeda agenda and Axeda Desktop server.

Fifth, in April 2022, Health-ISAC worked with Microsoft and others to take down the Zloader malware family, one of the most notorious cybercrime operations responsible for ransomware attacks against hospitals in the United States and around the world. The takedown was accomplished through coordinated legal and technical actions and disrupted massive botnets using the Zloader malware family, striking a major blow against cybercriminal operators using Ransomware, such as Ryuk, to extort victims.

With the seizing of hundreds of domain names used by the Zloader malware to remotely command and control victim computers, Microsoft will use the intelligence

gained from this takedown to partner with Law Enforcement, Internet Service Providers and Computer Emergency Response Teams around the world to help remediate infected computers, making the Internet safer for consumers and businesses worldwide. Together, these aspects of the operation are expected to undermine the criminal infrastructure that relies on these botnets every day to make money and helps to provide new tools for the industry to work together to proactively fight cybercrime.

At Health-ISAC, our mission is much bigger than the ISAC. We believe building a stronger community both inside and outside of the sector leads to better patient care and a healthier world.

Health Sector Coordinating Council Cybersecurity Working Group

Background

Healthcare is designated under U.S. national policy as "critical infrastructure" along with 15 other industry sectors, such as financial services, energy, telecommunications, water, transportation and more, represented by industry-organized "Sector Coordinating Councils (SCCs)." These SCC's and their government counterparts form a national public-private partnership coordinated overall by the U.S. Department of Homeland Security through the National Infrastructure Protection Plan (NIPP). The Health Sector Coordinating Council (HSCC) serves as an official advisory council to its government counterparts—HHS and FDA—with a formally designated critical infrastructure protection function distinct from the advocacy and member services roles of traditional industry associations. The HSCC, HHS and FDA work jointly to identify and mitigate systemic threats to critical healthcare infrastructure, such as pandemics, major weather events, terrorism, active shooters, and cyber-attacks, with a mission to identify cyber and physical risks to the security and resiliency of the sector, develop guidance and policies for mitigating those risks, and facilitate threat preparedness and incident response. The Office of the White House National Cyber Director has identified and engaged the HSCC as a model to accelerate a national healthcare cyber resilience strategy.

The HSCC Cybersecurity Working Group (CWG) is a volunteer coalition of 320 organizations that operate under a charter-based governance structure with an elected Chair, Vice-Chair and Executive Committee. Membership is open to any organization that is; (a) a covered entity or business associate under HIPAA; (b) a Health plan or payer; (c) regulated by FDA as medical device or pharmaceutical company; (d) regulated by HHS Office of the National Coordinator as a Health IT company; (e) a public health organization and (f) a healthcare industry association or professional society. A small allotment of an "Advisor" member category of consulting and security companies is permitted to participate and support CWG initiatives pro-bono.

When working with our government partners, the industry-led Cybersecurity Working Group becomes the *Joint* Cybersecurity Working Group, which identifies and develops preparedness measures against cybersecurity threats to the security and resiliency of the Health sector. It is organized into outcome-oriented task groups (currently 13) that meet regularly to develop best-practices for various healthcare cybersecurity disciplines such as 405(d) Health Industry Cybersecurity Practices, Supply Chain Cyber Risk Management, Five-Year Plan, Emerging Technology, Workforce Development, Measurement, Policy, Outreach and Awareness and Risk Assessment and Medical Technology Security including sub-groups around the Joint Security Plan Update, MedTech Legacy Devices, and MedTech Vulnerability Communications.

The CWG has produced 15 major best-practices publications since 2019, freely available to sector stakeholders and the public via its website (*HealthSectorCouncil.org*). These publications include *Health Industry Cybersecurity Practices, Health Industry Cybersecurity Tactical Crisis Response Guide, Health Industry Cybersecurity Securing Telehealth and Telemedicine, Model Contract Language for Medtech Cybersecurity Medtech Vulnerability Communications Toolkit* and *Operational Continuity Cyber Incident*.

Many of these HSCC CWG task group initiatives and deliverables directly address the many important recommendations contained in the 2017 HHS report of the Health Care Industry Cybersecurity (HCIC) Task Force, which was established by the Congress in Section 405(c) of the 2015 Cybersecurity Information Sharing Act and was composed of industry and government experts in healthcare and cybersecurity. At the time, the report characterized the healthcare industry's cybersecurity preparedness as being "in critical condition." As the Health Sector Coordinating

Council has been focused on developing cybersecurity best practices and tool kits—by the sector, for the sector—we hope that as more healthcare organizations implement these scalable practices over time, we will raise the sector's preparedness diagnosis to "stable." But in the business of cybersecurity, we are never done, only better.

To support the development of these initiatives, our preparedness, information sharing and incident response, both Health-ISAC and the HSCC CWG work closely with HHS and FDA, both of which serve as our CWG co-chairs and Sector Risk Management Agency (SRMA), as well as, CISA. Our ongoing partnership engagement includes holding weekly calls with the leadership in each organization to assess and discuss issues facing the sector.

The Cyber Threat Landscape in Healthcare

Ten years ago, 'cyber' and 'healthcare' were not even placed in the same sentence. Today because of the rise in digital healthcare, the proliferation of advances in technology and the efficiencies of connecting devices and data, the cyber threat surface in healthcare has ballooned and the threat actors have followed. Threat actors have many motivations to attack whether for financial reasons, disruption, intellectual property theft, revenge or to make a political statement.

Unfortunately, the stakes are very high. The focus has traditionally been on data and privacy but if HDOs, providers, or their suppliers cannot deliver services, as was seen in numerous ransomware attacks, or data is manipulated or destroyed, patient lives can be at risk.

There are essentially five malicious actor groups that are responsible for threats to healthcare, which include Nation States such as Russia and China, Cyber Criminals, Hacktivists, Terrorists, and Insiders who can be malicious or non-malicious. Their motivations range from **Advantage**—intellectual property theft, gain a foothold for further disruption, espionage, blackmail—**Ego**—notoriety, revenge—**Ideology**—political, social, cultural and **Greed**—money, power.

The various actor groups use several Tactics, Techniques and Procedures (TTPs) to conduct their activity. Some TTPs are Phishing and Spearphishing, Ransomware, Wipers, Distributed Denial of Service (DDoS), Business Email Compromise, Remote Access, Supply Chain Attacks, Scanning and Exploiting Vulnerabilities, Social Engineering and Credential Theft.

In November 2021, Health-ISAC conducted a survey of its members asking them to rank order the Top 5 "*greatest cybersecurity concerns*" facing their organizations for both 2021 and 2022. The survey included cyber (e.g., CISO) and non-cyber executives (e.g., CFO), multiple healthcare subsectors (e.g., Providers, Pharmaceutical Manufacturers, Payers, Medical Device Manufacturers, Health Information Technology), as well as, healthcare organizations of varying sizes and budgets. The Top 5 threats, which were the same for both 2021 and 2022 were:

1. Ransomware Deployment
2. Phishing/Spear-Phishing Attacks
3. Third-Party/Partner Breach
4. Data Breach
5. Insider Threat

Ransomware has had a big impact on the Health sector and threat actors have evolved their techniques over the last 2 years from simply just asking for a payment to unlock files to blackmailing organizations with threats to release records to the public. According to the Federal Bureau of Investigation (FBI) Internet Crime Complaint Center's (IC3) 2021 *Internet Crime Report*, the Health sector experienced at least 148 ransomware attacks between June 2021 and December 2021 resulting in millions of dollars of losses.

Ransomware family groups that have been particularly prolific in the healthcare sector include Conti and its Ryuk Ransomware. Ryuk has been linked to more than 200 ransomware attacks impacting hospitals, public health departments, nursing homes and patient care facilities around the world since 2018. The attacks resulted in the temporary or permanent loss of IT systems that support many of the provider delivery functions in modern hospitals resulting in canceled surgeries and delayed medical care. Some examples of impacts caused by Ryuk at patient care facilities in the United States since 2018 include:

- Ryuk attack forced ambulances to divert, causing a 90-minute delay in emergency patient services.

- Ryuk disrupted delivery of chemotherapy treatments for cancer patients.
- Ryuk forced hospitals to cancel elective procedures.
- Ryuk caused delays in reporting of laboratory results.
- Ryuk caused delays in scheduling appointments for maternity and oncology patients.
- Ryuk caused more than 3 weeks of downtime for the Electronic Health Records management system.
- Ryuk impacted systems at nursing homes, causing patient records to be unavailable and prohibiting pharmaceuticals orders from being placed, and
- Ryuk leaked sensitive patient data including treatments, diagnoses, and other information of hundreds of thousands of people.

Hospitals reported revenue losses due to Ryuk infections of nearly $100 million from data Health-ISAC obtained through interviews with hospital staff, public statements, and media articles. The Ryuk attacks also caused an estimated $500 million in costs to respond to the attacks—costs that include ransomware payments, digital forensic services, security improvements and upgrading impacted systems plus other expenses. A high-profile attack as the result of Conti/Ryuk was against the Health Service Executive (HSE), the national health system in Ireland consisting of 54 hospitals, in May 2021. The attack brought all the IT systems within HSE nationwide down and it took 4 months to completely recover from the incident.

Other Ransomware families are REvil/Sodinokibi, Hive, Lokibot, Pysa and Clop. Health-ISAC assesses that in 2022, Ransomware will continue to proliferate, and cybercriminals will target critical systems to the operations of healthcare organizations to force healthcare organizations to pay a ransom quickly and not allow time for investigation or forensic examination prior to paying the ransom demanded.

The other impact of Ransomware is the downstream effects that result when suppliers are attacked. When Kronos, a Human Resources Management Solutions firm widely used in healthcare, was attacked in December 2021, numerous hospitals were impacted. Hospitals were forced to manage payroll, staff scheduling, and issuing staff IDs manually during a surge in COVID–19 infections. In January 2021, when WestRock, a packaging solutions manufacturer that was essential in providing packaging for COVID–19 vaccines, treatments, and diagnostics, was hit with a Ransomware attack, pharmaceutical manufacturers were impacted by slowdowns in package production and shipping during a vital period in the pandemic.

The COVID–19 Pandemic was a factor in several incidents that took place over 2020 and 2021. Nation State activity has always been present in the sector, but it was especially visible during the COVID–19 pandemic with the desire to gain knowledge about vaccines, diagnostics and therapeutics related to COVID–19. Threat actors accessed documents covering the regulatory submission for Pfizer and BioNTech's COVID–19 vaccine candidate BNT162b2 at the European Medicines Agency (EMA) where the documents had been stored on EMA's servers. There were also several incidents such as when threat actors attacked and blocked access to an Italian COVID–19 vaccination booking system. Other activities targeted organizations offering cold storage and delivery processes for keeping vaccines at safe temperatures with phishing and spear-phishing campaigns.

A concerning threat actor trend has been the intention and ability to target IT providers, Managed Service Providers and Enterprise Management Software Systems to gain access to a larger group of victims. For example, in February 2020, threat actors affiliated with Russia's SVR (foreign intelligence service) injected malicious code into an update for SolarWinds Orion, a network monitoring software used by several organizations including the U.S. Federal Government. The malicious code went undetected until December 2020 and infected over 18,000 machines through the supply chain. Other high profile supply chain compromises included Kaseya and Accenture. Likely heading into 2022 threat actors will evolve this tactic and focus on compromising cloud providers to gain access to the sensitive data and networks of multiple victims.

Vulnerabilities also posed a huge problem for the sector. According to a graph published by the National Institute of Standards and Technology (NIST), vulnerabilities increased for a fifth straight year with 18,378 reported in 2021. Of that number, 3,646 were considered high-risk. Of particular note were the PrintNightmare vulnerability, the Microsoft Exchange Proxy Shell Attack vulnerability, and the Apache Log4j vulnerability which had very broad implications across the sector.

In 2022 there has been increased focus on Nation State activity and related criminal cyber activity surrounding the geopolitical events occurring between Russia and Ukraine. Many fear a fall-out from Russian activities against Ukraine such as what occurred during the 2017 Petya/Not Petya attacks that impacted over 300 companies, many of which were large multi-national corporations, and cost over $10 billion. Recent reporting shows Russian threat actors attacked Viasat, a US provider of high-speed satellite broadband services, 1 hour before Russia invaded Ukraine. Thousands of satellite terminals were affected impacting myriad internet users in Europe as well as over 5,800 wind turbines producing electricity. Even if healthcare is not directly targeted, cascading impacts such as access to communications and electricity can be substantial. Health-ISAC assesses that threat actor cyber activities will continue to rise and evolve, and the sector needs to be ever vigilant, as well as, develop robust enterprise risk management and resiliency strategies.

The Unique Nature of Healthcare

The Health sector is highly inter-connected. Unlike in other sectors, healthcare data must be portable. Sensitive patient information must move between various medical providers, pharmacies, diagnostic facilities, and payers to facilitate proper patient care and history, as well as, payment for those services. Many healthcare facilities such as hospitals operate in environments that are accessible to the public. Hospitals employ tens of thousands of medical devices, many using outdated operating systems, and many of which are connected to a network. These devices are made by a variety of manufacturers with various levels of security and patching protocols built in. Expensive equipment such as Magnetic Resonance Imaging (MRI) machines are not easily replaced and run on software that is no longer patched or supported. In addition, many of these devices run 24 hours a day, 7 days a week, 365 days a year, so taking them offline for patching or other security needs is complicated.

When supply chains are tightened or non-existent for various reasons, or pandemics or natural or man-made regional disasters occur, stretched supplies and staff become an additional factor.

Coupled with a diverse base within the sector, a highly regulated environment, complex siloed departments, a lack of skilled cyber staff, a lack of cyber security situational awareness, a lack of knowledge and training for the medical staff as well as at the CEO and Board level, and lack of cyber security strategy including a risk management approach, the Health and Public Health sector faces enormous challenges.

Meeting the Challenge

Despite the numerous challenges, many organizations in the Health sector have taken great strides to make certain their environments are as protected and resilient as they can be. As can be seen by the contributions of the Health Sector Coordinating Council Cybersecurity Working Group and Health-ISAC, countless individuals dedicate numerous hours of their time to help ensure the sector is strong and secure. Both the HSCC CWG and Health ISAC have robust communities that thrive on collaboration in their mission. As is the tradition in medicine, members of these two organizations truly care about patient welfare and safety and the protection of the ecosystem that contributes to them. Members share best practices, indicators of compromise, mitigation strategies and other vital information to accomplish this. When the Petya/Not Petya attacks of 2017 took place, some 60 individuals of approximately 34 Health-ISAC member firms came together and within 48 hours, determined what the actual attack was, the attack vector, how it spread and how to stop it and the shared their findings not just within the sector but globally via the Health-ISAC website and alerts. The publications produced, webinars and workshops held, exercises conducted and TLP WHITE alerts are open to the sector and are free. In 2021, Health-ISAC delivered targeted alerts to 49 healthcare companies that were non-members. The Zloader takedown will benefit countless organizations inside and outside of the sector and industry is looking to do more in this space.

Despite the number of great initiatives and efforts underway within the sector, the sector needs to be vigilant. We can no longer look at the challenges through just a cyber-or physical security lens, but must employ enterprise risk management to consider all threats to operational resilience. As evidenced by Hurricane Maria in Puerto Rico and its impact on the availability of IV bags, ransomware attacks on healthcare and healthcare suppliers, which have crippled healthcare delivery, the COVID–19 shutdown in Shanghai that has tightened the supply of contrast fluid used for imaging, which has forced physicians to prioritize which patients can get

CT scans, MRIs and more, healthcare organizations must constantly be focused on all threats to healthcare delivery and patient safety. The healthcare sector should be supported and incentivized in this vital effort.

Congress can help meet this challenge by focusing on three key areas:

(1) EDUCATION, RECOGNITION AND FACILITATION OF THE IMPORTANCE OF INFORMATION SHARING

One of the greatest challenges for Health-ISAC and all ISACs is the lack of awareness amongst the critical infrastructure owners and operators, particularly the smaller owners and operators, that the ISACs and SCCs exist and have valuable tools available to improve security—many of which are free to use. Numerous incidents have shown that effective information sharing amongst robust trusted networks of members works in combatting cyber threats.

Government, and specifically the SRMAs should regularly and consistently encourage owner/operators and especially at the Board and CEO level to join their respective ISACs and Sector Coordinating Councils. This has been very effective in the financial sector where the United States Department of the Treasury, the regulators and state agencies have been strongly encouraging membership in the FS-ISAC as a best practice.

The SRMAs indeed have a policy reference for this kind of advisory to their sector representatives: the NIST Cybersecurity Framework. This Framework, developed over the course of a year collaboratively by government and private sector stakeholders, lays out a cyber risk management framework linked to five core functions: identify, protect, detect, respond, and recover. Among the functional categories identified as part of a mature cyber risk management strategy is external communications and coordination around cyber security threats, response, and best practices. In other words, membership in an ISAC or ISAO and/or the SCC is an essential element of a successful cyber risk management strategy.

Another way to facilitate sharing and build robust communities is by providing financial incentives through tax breaks or other means to critical infrastructure organizations that join their respective ISACs and/or SCCs.

(2) PROVIDE INCENTIVES FOR ADOPTION OF CYBERSECURITY BEST PRACTICES

Cyber threat actors are agile, in many cases run their operations as businesses, are sophisticated and constantly evolve their TTPs to infiltrate an organization's defenses and achieve their goal. It is much easier to attack versus defend and healthcare organizations are often at a disadvantage, especially smaller organizations that do not have financial and infrastructure resources. Due to the huge growth in cybercrime and large ransomware payouts, sophisticated and organized criminal groups will be able to invest heavily into R&D and develop new ways to conduct automated and effective scams. The criminals will leverage machine learning, artificial intelligence, and deep fakes to perpetrate efficient and effective criminal campaigns. Therefore, it is essential to support healthcare organizations by incentivizing them to adopt at a minimum basic cybersecurity and risk management strategies. Some good best practices include employing multi-factor authentication (MFA) and other access controls, having a layered defense, using endpoint security, developing network segmentation, building prevention and detection strategies, backing up data and training staff on cyber impacts and policies.

(3) ESTABLISH CYBER SECURITY PROFESSIONALS AS SRMA LIAISONS

With the challenging nature of the Health sector and the steady rise in cyber threats and incidents, there should be a cyber security professional within HHS to act as a strong, government liaison and advocate for the public private partnership when it comes to cyber matters. It has become increasingly apparent that industry needs a government representative who understands cyber security issues, threats, vulnerabilities and impacts as well as the blended threats between physical and cyber security. Having an established, clear government 'go-to' lead in this area is imperative to strengthening the partnership and improving the overall cyber security posture of the Health and Public Health sector.

This concludes my testimony. Thank you again for the opportunity to present this testimony and I look forward to your questions.

[SUMMARY STATEMENT OF DENISE ANDERSON]

The testimony will provide descriptions of Health-ISAC, ISACs in general, and the Health Sector Coordinating Council Cybersecurity Working Group, including the numerous initiatives that are taking place within industry to help secure the sector and keep it resilient in the face of threats. It will look at the cyber threat landscape in healthcare and will include the major threat actor groups, threat actor motivations, as well as, threat actor Tactics, Techniques and Procedures (TTPs). The testimony will provide a summary view of the top five "*greatest cybersecurity concerns*" Health-ISAC members see facing their organizations for both 2021 and 2022. Also covered are Ransomware, downstream impacts of Ransomware, Supply Chain attacks, vulnerabilities, and Nation State activity—especially related to COVID–19 and the development and distribution of vaccines, diagnostics, and therapeutics, as well as the recent geopolitical tensions between Russia and Ukraine. The unique nature of healthcare and its myriad challenges, such as the necessity of portable data, 24-by–7-by 365 operations, equipment and devices that are no longer supported, but not easily replaced, reliance upon other critical infrastructure and supply chains, all exacerbated when pandemics, natural and man-made events take place, will be described. Finally, three suggestions are made where Congress and Government can help the Health sector in its efforts to improve security and resilience.

The CHAIR. Thank you very much.

Mr. Corman.

STATEMENT OF JOSHUA CORMAN, FOUNDER, I AM THE CAVALRY, DOVER, NH

Mr. CORMAN. Chair Murray, Senator Cassidy, distinguished Members of the Senate Health Committee, thank you for the time to speak to you today about some pretty grave matters that weigh heavy on my heart——

The CHAIR. Is your mic on?

Mr. CORMAN. I will try that again.

The CHAIR. Very good.

Mr. CORMAN. Chair Murray, Senator Cassidy, and distinguished Members of the Senate Health Committee, thank you for the opportunity today to talk about these grave matters that weigh heavy on my heart.

As described, I am Josh Corman. I am the founder of a volunteer grassroots group of hackers trying to save lives through security research. In recognition that the cavalry isn't coming, we asked, what are you willing and able to do? Will you be part of that solution? Will you be a voice of reason and technical literacy and a helping hand to work with policymakers such as yourselves to make things safer?

Our problem statement was simple, our dependence on connected technology was growing faster than our ability to secure it in areas affecting public safety, human life, and National Security. What we were doing 9 years ago was trying to build the trust and the foundation so that we could prevent loss of life.

There is a promise in a parallel to connect to technology. We always adopt things that are immediate and obvious benefits. We have a very hard time determining the delayed consequences of those choices. And I warned the teams, people would have to die first before anyone would listen to us.

To our delight and surprise, bravery from Dr. Suzanne Schwartz at FDA took bold action to try to make sure we raised the bar for

minimum cybersecurity hygiene for medical devices and issued the first ever safety communication for a medical device purely for cybersecurity reasons and no one had died. They sent a shot over the bow to the industry of 10,000 medical device makers that the dependence we place on connected technology should be worthy of that trust.

These are devices like this little pacemaker, some of which have found a sync—a hardcoded three digit password is sufficient to affect the hearts and functions of 750,000 patients. We have similarly compromised insulin pumps to give a second lethal dose of insulin without authentication done by a diabetic himself. We have found bedside infusion pumps that should deliver a 3-hour dose of a calcium channel blocker could empty the contents in 30 seconds.

We have done these through clinical E.R. hacking simulations in consultation and collaboration with Federal agencies, with medical practitioners, with physicians to see, can we handle these disruptions to the technologies we take for granted? Through that work, I got to serve on the 2015 405c Congressional Task Force on Health Care Industry Cybersecurity.

Because of the trust built there, when the country and the world faced the pandemic of the COVID–19 virus, Director Krebs, using the Cares Act hiring authority, asked me to serve my country and design and implement what became this as a COVID task force. Senator Cassidy, that report that you referred to, we looked harder and closer at the ability, the Nation's ability to provide medical care than anyone had before. And armed with the extreme pressures and strains of the pandemic, we could use data science to calculate how ICU strain dramatically caused loss of human life.

We found that if the country's ICU beds hit 75 percent, you would see 18,000 lost Americans in 2 weeks with additional amounts four and 6 weeks later. And if you hit 100 percent ICU strain, you would see 80,000 lost Americans. And unlike the losses to COVID, these were 25 to 44 year olds primarily.

The question became, can these cybersecurity failures affect patient care and human life? And we were able to determine the answer was yes. Delays in integrated care affect mortality rates. The seminal New England Journal of Medicine article showed that a 4.4 minute longer ambulance ride during a U.S. marathon had a statistically significant impact on mortality rates 30 days later. Similarly, with strokes, the golden hour or golden hours is one, three, or 4 hours can affect patient care, if you can walk again, if you can talk again.

A 4.4 minutes can affect the mortality for heart. And 4 hours is the difference between life and death for brain. What do 4 weeks of downtime for the State of Vermont or for the protracted impacts to Scripps Health Care in San Diego? These failures further strained already record strained health care delivery, introducing a loss of life, not just of elderly with 65 years or four or more comorbidities, but critical infrastructure aged workforce that we depend upon, and in parallel with these record high strains, as these losses of life succumb to COVID, non-covid conditions, injury, burnout, retirement, and alterations to their family support structure.

If we zoom out to Maslow's hierarchy of needs, in the last 2 years, we have seen successful compromises of the water we drink, the food we put on our table, the oil and gas that fuels our cars in our homes, the schools our children attend, the municipalities who run our towns or our cities, the timely access to patient care during a pandemic. I myself suffered degraded and delayed care, which imperiled my ability to serve the country during these 2 years.

We are overdependent on the panel things and while we are doing many correct things and this body themselves have taken bold action, these voluntary practices where we take our time have not proven sufficient to transcend the market failures. The adversaries are setting the pace.

We are messing with Maslow. It is not tenable for an individual nor a nation. And with the threats or further attacks from Putin and other nations or adversaries, we need bold action, and we need it now. Any crisis of confidence in the public to trust these baseline functions is unacceptable. We need to be better. We have a head start.

I have in my testimony areas where we can stem the bleeding in the foreseeable future, but it will take much more substantive action. I look forward to answering your questions.

[The prepared statement of Mr. Corman follows:]

PREPARED STATEMENT OF JOSHUA CORMAN

Opening:
Chair Murray, Ranking Member Burr, and distinguished Members of the Senate Committee on Health, Education, Labor, and Pensions, thank you for the opportunity to testify today.

My name is Joshua Corman. I am a Philosopher, Hacker, Protector, and Puzzler… driven to make the world a safer place. Nearly 9 years ago, I founded "I am The Cavalry" (dot org) - a volunteer, cyber safety initiative focused on public safety and human life in the internet of things – or as we like to say: *"where Bits & Bytes meet Flesh & Blood"*. Most recently, I designed and drove what became the *CISA COVID Task Force* (under the CARES Act emergency hiring authority). I am an adjunct faculty for the CISO Certificate Program at Carnegie Mellon University's Heinz College. Lastly, I testified to the *2016 Presidential Commission on Enhancing National Cybersecurity*[1] and served on the (405c) *Health Care Industry Cybersecurity Task Force*[2] – initiated by Congress in the Cybersecurity Act of 2015.

Bottom Line Up Front:
Attacks on healthcare are increasing in volume, variety, and impact - with consequences now include the loss of life. While directionally-correct steps have been taken, we're getting worse faster than we're getting better. Bold actions and assistance will be required to change this trajectory, address these market failures, lack of incentives, and historical under-investments.

I'd like to bring you good news. However, the more consequential the subject matter, the more important it is to be forthright and avoid exaggeration in either direction. The candid truth is, I am more concerned about the cybersecurity of US healthcare than I ever have been.

Note: For events which occurred during my emergency Federal service (which ended January 14, 2022), I will err on discussing public and/or published materials.

Attackers have gotten stronger, but defenders have not - and many got weaker. The number of healthcare attacks have grown. The costs of the ransom payments have grown.[3] The impact of attacks are no longer merely measured by record count, fines, ransom payments, or recovery costs… but including double-digit millions of lost revenue and worse… degraded patient care and human life.[4] Crisis adjustments, made in a

---

[1] 2016 Presidential Commission on Enhancing National Cybersecurity
https://www.nist.gov/system/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf
[2] Health Care Industry Cybersecurity Task Force Report
https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf.
[3] RTF Report: Combating Ransomware - A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force
https://securityandtechnology.org/ransomwaretaskforce/report/
[4] CISA Insights Provide Medical Care is in Critical Condition: Analysis and Stakeholder Decision Support to Minimize Further Harm
https://www.cisa.gov/sites/default/files/publications/CISA_Insight_Provide_Medical_Care_Sep2021.pdf..

hurry, added more technologies and attack surfaces. Financial constraints have forced reduced investments in cybersecurity staff and operating budgets.

The majority of healthcare regulations have focussed on the confidentiality of records. However, "**Cyber Safety is Patient Safety**". I love my privacy; I'd like to be alive to enjoy it. Yes, defensible connected technologies will require investment - as will the talent to defend them. Scrubbing-in before surgery takes time/money – *and* this vital hygiene practice dramatically reduces post-op infection, complications, and mortality rates. As technology increasingly plays a role in the delivery of modern healthcare, cyber-hygiene is no longer negotiable. While many have exclaimed they can't afford to do more, I tried to channel my inner Stan Lee: With Great Connectivity, Comes Great Responsibility…

With seams and cracks in healthcare noted in our 2017 405c report,[5] the pandemic widened and shattered those issues for many.

The pandemic brought an untenable, perfect storm of a record high need for patient care in the face of record high adversary activity, and severely diminished resources with which to defend the healthcare delivery environments.[6]

Degraded and delayed care affects patient outcomes.[7] Cybersecurity disruptions can cause and exacerbate delays and degrade care for a hospital, town, region, or even at the state level.[8]

Zooming out, while the country has 16 designated critical infrastructure sectors - with 55 National Critical Functions spanning them - Healthcare and "provide Medical Care" during the pandemic may be respective first among equals. Overall pandemic strains have not merely affected the general population, but have had material impact to the skill-workers and the critical infrastructure workforce that support foundational, life-line critical functions that underpin society (food, water, power, transportation, and brittle supply chains, etc.). As the CISA COVID Task Force came to an end in January, I was alerting CISA, the White House, Federal and Private Sector leadership of material erosions (10, 20, and 30%) to critical infrastructure workforce and difficult-to-replace skill workers - as they succumb to: death from COVID, death from non-COVID, injury, burnout, retirement, and alterations to their family support structure.

Adversaries are disrupting the bottom of Maslow's Hierarchy of Needs.[9] Insecurity at the

---

[5] Health Care Industry Cybersecurity Task Force Report https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf.
[6] Ransomware Hits Dozens of Hospitals in an Unprecedented Wave https://www.wired.com/story/ransomware-hospitals-ryuk-trickbot/.
[7] Delays in Emergency Care and Mortality during Major U.S. Marathons https://www.nejm.org/doi/full/10.1056/nejmsa1614073.
[8] Hospitals say cyberattacks increase death rates and delay patient care https://www.theverge.com/2021/9/27/22696097/hospital-ransomware-cyberattack-death-rates-patients.
[9] Maslow's hierarchy of needs https://en.wikipedia.org/wiki/Maslow%27s_hierarchy_of_needs.

base of his famous pyramid is not tenable for an individual - and certainly not sustainable for a country. Do not mess with Maslow…

Context:
My sentiment below becomes more true with each passing year:

> ***Through our over dependence on undependable IT, we have created the conditions such that the actions of any single outlier can have a profound and asymmetric impact on human life, economic, and national security.***

When I first wrote this, my hope was to prevent high consequence failure in cyber-physical-systems and critical infrastructure. Yet over the last 2 years, we have seen successful attacks and disruptions to:

- The *water* we drink[10,11]
- The *food* we put on our tables[12,13,1415]
- The *oil & gas* that fuels our cars and our homes[16]
- The *schools* our children attend[17,18,19]
- The timely *access to patient care* - with mortal consequences - during the strains of a pandemic[2021]

---

[10] A Hacker Tried to Poison a Florida City's Water Supply, Officials Say https://www.wired.com/story/oldsmar-florida-water-utility-hack/.
[11] Hackers Tried to Poison California Water Supply in Major Cyber Attack https://www.newsweek.com/san-francisco-water-plant-hack-cyber-attack-poison-supply-1601798.
[12] Ransomware Hits a Food Supply Giant—and Underscores a Dire Threat https://www.wired.com/story/jbs-ransomware-attack-underscores-dire-threat/.
[13] Ransomware gang strikes Iowa agriculture business New Cooperative, the latest hack on food supply chain https://www.cyberscoop.com/blackmatter-new-cooperative-ransomware-iowa/.
[14] 'Cyber event' knocks dairy giant Schreiber Foods offline amid industry ransomware outbreak https://www.cyberscoop.com/schreiber-foods-cyber-event-ransomware-agriculture-food/.
[15] AGCO's business operations disrupted by ransomware attack https://www.securitymagazine.com/articles/97576-agcos-business-operations-disrupted-by-ransomware-attack.
[16] Hackers Breached Colonial Pipeline Using Compromised Password https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password.
[17] Ransomware Has Disrupted Almost 1,000 Schools in the US This Year https://www.vice.com/en/article/4awyvp/ransomware-has-disrupted-almost-1000-schools-in-the-us-this-year.
[18] Texas, California, New York, Louisiana, Missouri lead list of states with most ransomware attacks on schools: report https://www.zdnet.com/article/texas-california-new-york-and-louisiana-missouri-lead-list-of-states-with-most-ransomware-attacks-on-schools-report/.
[19] Hackers prey on public schools, adding stress amid COVID pandemic - Albuquerque, NM https://www.pbs.org/newshour/education/hackers-prey-on-public-schools-adding-stress-amid-covid-pandemic.
[20] Patients of a Vermont Hospital Are Left 'in the Dark' After a Cyberattack https://www.nytimes.com/2020/11/26/us/hospital-cyber-attack.html.
[21] Ransomware Attack Hits Universal Health Services https://www.wsj.com/articles/ransomware-attack-hits-universal-health-services-11601341873.

- The *municipalities* who run our towns and our cities[22,23,24]
- ….even *Federal agencies* charged with public safety and national security…[25,26]

…stuff… is on fire…

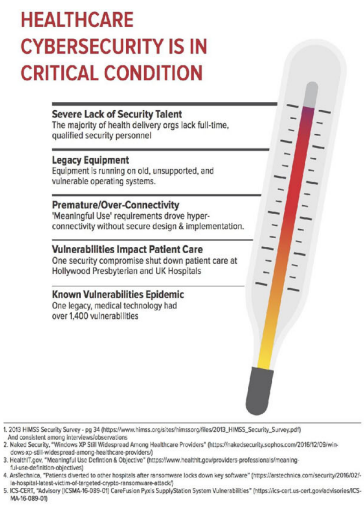
We were prone. We were prey. Our predators finally noticed. Their largely-unchecked aggression has emboldened them. With blood in the water from the strains of the pandemic, healthcare found itself in a feeding frenzy.

Escalation over the last few years in Healthcare:
In early 2016, because of hard-earned trust built between I am The Cavalry and the FDA,[27] I had the privilege to serve on the CISA 2015 405c Congressional Task Force on these matters.[28] Our task force started shortly after an untargeted SamSam ransomware hit Hollywood Presbyterian Hospital in LA - diverting ambulances to other facilities, canceling surgeries, and even moving critical care patients.[29] It ended near Mother's Day weekend 2017 with WannaCry wreaking havoc on UK healthcare - manifesting many of our worst fears.[30] Prior to knowing this would happen, the banner graphic in our report to congress earlier that week stated bluntly:

"HEALTHCARE CYBERSECURITY IS IN CRITICAL CONDITION"

---

[22] Amid a surge in ransomware attacks, cities are taking some of the biggest hits https://www.washingtonpost.com/politics/amid-a-surge-in-ransomware-attacks-cities-are-takingsome-ofthe-biggest-hits/2021/09/02/9bd5d654-0a84-11ec-aea1-42a8138f132a_story.html.
[23] Hackers have been holding the city of Baltimore's computers hostage for 2 weeks https://www.vox.com/recode/2019/5/21/18634505/baltimore-ransom-robbinhood-mayor-jack-young-hackers.
[24] Four months on from a sophisticated cyberattack, Alaska's health department is still recovering https://www.zdnet.com/article/four-months-on-from-sophisticated-cyber-attack-alaskas-health-services-is-still-recovering/.
[25] DHS, DOJ And DOD Are All Customers Of SolarWinds Orion, The Source Of The Huge US Government Hack https://www.forbes.com/sites/thomasbrewster/2020/12/14/dhs-doj-and-dod-are-all-customers-of-solarwinds-orion-the-source-of-the-huge-us-government-hack/?sh=a170ec825e68.
[26] Suspected Russian hackers spied on U.S. Treasury emails - sources https://www.reuters.com/article/us-usa-cyber-amazon-com-exclsuive/exclusive-u-s-treasury-breached-by-hackers-backed-by-foreign-government-sources-idUSKBN28N0PG.
[27] Hippocratic Oath for Connected Medical Devices https://iamthecavalry.org/issues/medical/oath/.
[28] Health Care Industry Cybersecurity Task Force Report https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf.
[29] Ransomware takes Hollywood hospital offline, $3.6M demanded by attackers https://www.csoonline.com/article/3033160/ransomware-takes-hollywood-hospital-offline-36m-demanded-by-attackers.html.
[30] NHS could have avoided WannaCry hack with 'basic IT security', says report https://www.theguardian.com/technology/2017/oct/27/nhs-could-have-avoided-wannacry-hack-basic-it-security-national-audit-office.



Almost exactly five years later, the situation has grown much more severe.[31] Without bold leadership and swift action, I fear we're not yet to the worst of it.

In June of 2017, while in Tel Aviv CyberWeek explaining to our UN counterparts how lucky we all got with WannaCry, Russia's NotPetya escaped its intended blast radius of Ukraine causing more than $10B of damage worldwide - with $1B alone to Merck Pharmaceuticals.[32] It was at that time that I challenged that international policy cohort to consider a "Cyber-No-Fly-Zone" on at least hospitals (chronicled in the *Sandworm* book).[33] I argued that harms from cyber-munitions against hospitals - intentional or otherwise - should be severely punished and sanctioned. While most allies are loath to enact norms or treaties about cyber-conflict, it is routinely discussed that attacks from a Nationstate, harming country-designated "critical infrastructure" could constitute an act of war.[34] NOTE: Healthcare is designated Critical Infrastructure.

---

[31] 5 Years That Altered the Ransomware Landscape
https://www.darkreading.com/endpoint/five-years-that-changed-the-ransomware-landscape.
[32] The Untold Story of NotPetya, the Most Devastating Cyberattack in History
https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.
[33] Sandworm by Andy Greenberg
https://www.penguinrandomhouse.com/books/597684/sandworm-by-andy-greenberg/.
[34] Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations
https://www.cambridge.org/core/books/tallinn-manual-20-on-the-international-law-applicable-to-cyber-operations/E4FFD83EA790D7C4C3C28FC9CA2FB6C9.

Over the next few years, the ransomware revolution grew bolder and more sophisticated, expanding their appetite to more types of prey.[35] The unavailability of what's important to *you*, can be made valuable to *them*.

As the pandemic reached US soil in early 2020, in the Sandbox at the RSA Conference, I warned then-Director Krebs that I expected a larger volume and variety of ransom attacks on hospitals. I offered a "director's cut" of our 2017 report to congress for him and his team - when the time was right. A few weeks later he called. He did not ask for the briefing. Instead, he asked if I would serve my country for a year. I'll next outline what happened over the next two years.

Cyber-Attacks during COVID-19:
As feared, unscrupulous threat actors started attacking hospitals and medical supply chains for vital and scarce supplies like Personal Protective Equipment (PPE).[36] Scores of volunteer cybersecurity do-gooders formed groups like the CTI League (Cyber Threat Intelligence League) to assist governments in identifying bad actor infrastructure.[37] CISA had already launched what they called PROJECT TAKEN to help hospitals (approximately 85% of whom lacked a single, experienced cybersecurity person on staff).[38,39] As I was being on-boarded through the CARES Act, the country was additionally organizing around what became Operation Warp Speed (OWS). Our eventual CISA COVID Task Force took responsibilities with both - across the interagency.[40]

In addition to engaging and attempting to protect OWS entities, my initial focus was prioritizing a long list of smaller, but potentially vital suppliers to the official OWS funded entities. Using a strategy I dubbed our "Ball Bearings" analysis… We spotted smaller, weak links in the vaccine supply chains who if disrupted could have a profound impact on American lives and interests.[41,42] A recurring uncomfortable reality was that most of these entities lacked even the most basic of cybersecurity. As was the case with healthcare delivery organizations (HDOs), these ball bearings were "*Target Rich, but Cyber Poor*". We were going to have to meet them where they are, and bring

---

[35] WSJ Mounting Ransomware Attacks Morph Into a Deadly Concern https://www.wsj.com/articles/mounting-ransomware-attacks-morph-into-a-deadly-concern-11601483945.
[36] PPE, COVID-19 Medical Supplies Targeted by BEC Scams https://threatpost.com/ppe-covid-19-medical-supplies-bec-scams/154806/
[37] CTI League https://cti-league.com/.
[38] US cyber officials try to channel Liam Neeson in responding to coronavirus threats https://www.cyberscoop.com/project-taken-liam-neeson-dhs-cybersecurity-coronavirus/.
[39] Health Care Industry Cybersecurity Task Force Report https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf.
[40] THE COVID-19 VACCINES WEREN'T HACKED — THIS TASK FORCE IS ONE REASON WHY https://www.theverge.com/2021/7/8/22568397/covid-vaccine-cybersecurity-cisa-task-force.
[41] CyberCast Season 3 Episode 18 - How CISA's COVID-19 Task Force Protected Hospitals and the Vaccine Supply Chain https://www.youtube.com/watch?v=gl40RaxCflk.
[42] Business Insider - Meet the government worker who cut through months' worth of federal bureaucracy in 10 days to help millions of Americans get vaccinated https://www.businessinsider.com/cisa-kenrda-martin-covid-vaccine-bureaucracy-2021-6.

fit-for-purpose methods to identify and buy down the risks that we could. This later became the foundation for what I've been calling the "*Pragmatic Security Suite*".

September saw an uptick in attacks on hospitals. The large, publicly traded hospital network known as UHS suffered a fairly serious ransomware attack.[43] This was my first big opportunity to work across the interagency. It was far more challenging than I was expecting. The good news: this was part of why the CARES Act was enacted – to help combine experience and skills to better serve the public throughout the pandemic. Given that UHS is publicly traded, several of the impacts were eventually disclosed - including a declared $67MM in lost revenue from the ordeal.[44,45]

While many across the healthcare sector discussed the growing impacts of records lost, fines levied, dollars paid to ransoms and restoration services, and now significant lost business… I began to fear that these service disruptions would be measured in degraded and delayed care, patient outcomes, and even lost lives.

Not long after the UHS experience, I helped to rally HHS, FBI, and CISA to issue a joint three-agency (Tri-Seal) Alert to warn the sector of a credible threat to disrupt plural US Healthcare entities concurrently - in close proximity to the US Presidential Election.[46] While we did our best to warn, far too many already strained hospitals fell victim to these more aggressive attacks. At the time, there were some who doubted the intelligence,[47] but in subsequent coverage and reporting from WIRED, the Wall Street Journal, and others… proved the intent to disrupt and intercepted communications reveal just how serious and perilous this was for the country.[48] These attacks felt at least state-tolerated… but more recent reporting suggests they were even state directed.[49] Not only are hospitals designated critical infrastructure, but they are also more taxed and strained than sustainable - without cyber-disruption.

Some victims of this campaign suffered severe and protracted effects on patient care. One such public example was in Vermont - covered in a harrowing story in the NYT.[50] In

---

[43] UHS Hospitals hit by Ryuk ransomware, forced to shut down systems https://www.securitymagazine.com/articles/93482-uhs-hospitals-hit-by-ryuk-ransomware-forced-to-shut-down-systems.
[44] Cyberattacks Cost Hospitals Millions During Covid-19 https://www.wsj.com/articles/cyberattacks-cost-hospitals-millions-during-covid-19-11614346713.
[45] United States Securities and Exchange Commission - United Health Services, Inc. https://www.sec.gov/Archives/edgar/data/0000352915/000156459022006717/uhs-10k_20211231.htm.
[46] Alert (AA20-302A) - Ransomware Activity Targeting the Healthcare and Public Health Sector https://www.cisa.gov/uscert/ncas/alerts/aa20-302a.
[47] Healthcare Providers Were Warned of a Ransomware Surge Last Fall. Some Still Aren't Sure How Serious the Threat Was https://therecord.media/healthcare-providers-were-warned-of-a-ransomware-surge-last-fall-some-still-arent-sure-how-serious-the-threat-was/.
[48] Ransomware Hits Dozens of Hospitals in an Unprecedented Wave https://www.wired.com/story/ransomware-hospitals-ryuk-trickbot/.
[49] Leaked Ransomware Docs Show Conti Helping Putin From the Shadows https://www.wired.com/story/conti-ransomware-russia/.
[50] Patients of a Vermont Hospital Are Left 'in the Dark' After a Cyberattack https://www.nytimes.com/2020/11/26/us/hospital-cyber-attack.html.

an attempt to assist future victims, the University of Vermont Medical Center eventually published a detailed report of how this attack affected their oncology capabilities.[51]

Major attacks would later degrade and delay care in other regions and states. After the Scripps attacks in San Diego, Dr. Christian Dameff began writing about how an attack on one hospital can drive significant surplus case loads onto proximal, alternative care facilities - with cascading effects.[52,53,54,55]

Excess Deaths and Loss of Life:
Delays affect mortality rates.[56] Cyberattacks can cause delays - big ones.[57]

In early 2021, I asked the team an uncomfortable question:
Can these cyberattacks contribute to loss of life?

With some analysis and data science, we were able to measure how they can.

The simplified abstraction is this:
Ransoms can strain hospitals to levels associated with Excess Deaths.[58]

We studied a state hit hard by ransomware - for a statistically significant observation period. In the same state, with the same population, during the same pandemic, controlling for hospital type and size, locations hit by ransom both achieved these excess death danger zones sooner and stayed there longer than their peers.

Sanitized versions of these models and methods were published in late 2021.

---

[51] JCO Oncology Practice: Cancer Care in the Wake of a Cyberattack: How to Prepare and What to Expect https://ascopubs.org/doi/full/10.1200/OP.21.00116.
[52] San Diego EDs Deluged With Patients After Cyberattack https://www.medpagetoday.com/meetingcoverage/acep/95357.
[53] Annals of Emergency Medicine - Research Forum Abstract: 108 Emergency Department Crowding Resulting from a Local Health System Cyberattack https://www.annemergmed.com/article/S0196-0644(21)00959-8/fulltext.
[54] Annals of Emergency Medicine - Research Forum Abstract: 7 Impact of a Hospital Cyberattack on EMS Arrivals at Neighboring Emergency Departments https://www.annemergmed.com/article/S0196-0644(21)00856-8/fulltext.
[55] Annals of Emergency Medicine - Research Forum Abstract: 162 Regional Emergency Department Census Impacts During a Cyber Attack https://www.annemergmed.com/article/S0196-0644(21)01014-3/fulltext.
[56] Delays in Emergency Care and Mortality during Major U.S. Marathons https://www.nejm.org/doi/full/10.1056/nejmsa1614073.
[57] Hospitals say cyberattacks increase death rates and delay patient care https://www.theverge.com/2021/9/27/22696097/hospital-ransomware-cyberattack-death-rates-patients.
[58] The Pandemic Revealed the Health Risks of Hospital Ransomware Attacks https://www.theverge.com/2021/8/19/22632378/pandemic-ransomware-health-risks.

On October 1st, CISA Published a collection of this analysis in a report called: *"Provide Medical Care Is In Critical Condition"*.[59] The Excess Death / Hospital Strain data science instrument was subsequently published on November 18th, 2021 in the CDC MMWR (Morbidity and Mortality Weekly Report) called "Impact of Hospital Strain on Excess Deaths During the COVID-19 Pandemic".[60] To make these dense reports more accessible, we recorded a short CISA Webinar as well.[61]

As CISA was about to publish our statistical evidence regarding loss of life, the Wall Street Journal published a front page story about a baby who died after a complicated birth at an Alabama hospital that had recently suffered disruptions from a cyberattack.[62]

A bit more on the Excess Deaths
The CISA COVID Task Force had been analyzing risks and system dynamics related to the National Critical Function (NCF) known as "Provide Medical Care". In February 2021, when the country hit the sobering milestone of 500,000 Americans lost to COVID,[63] we had also achieved an additional 150,000 Americans lost to what the CDC tracks as Excess Deaths. Excess Deaths are defined as the difference between expected deaths and actual deaths - by month, condition, and state. As we dug into the year of Excess Deaths, several things concerned us. Unlike COVID deaths affecting primarily 65+ year olds, 25-44 year olds were the fastest growing portion of these Excess Deaths. A review of the top causes revealed several time-sensitive conditions for which delayed access to care is known to affect mortality rates (heart, brain, pulmonary, etc). I know from my Cavalry and 405c Task Force work that, for example:

Even 4.4 minutes can affect mortality rates for heart attacks (NEJM)[64]
1-4 hours is critical to save brain/life with strokes; the Golden hour(s)

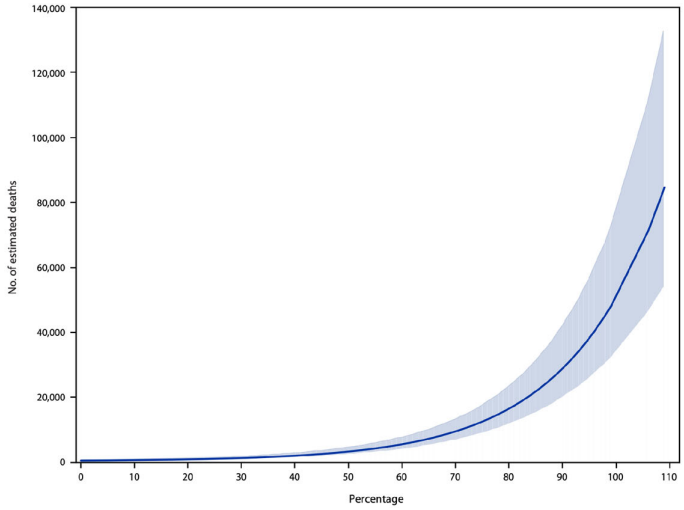
We chose to study these Excess Deaths more closely - and to hopefully find ways to mitigate these losses of life.

One of our findings was stunning. We found a strong positive correlation between Adult Intensive Care Unit (ICU) Bed utilization and Excess Deaths two, four, and six weeks later. In the model, if the country hit 75% ICU Bed utilization, you'd expect 18,000 lost Americans in two weeks. If the model hit 100%, it would indicate 80,000 lost Americans in two weeks. Delayed and degraded care affects outcomes for time sensitive conditions. ICU strain significantly added delays. Cyberattacks made them worse.

---

[59] CISA Insights Provide Medical Care is in Critical Condition: Analysis and Stakeholder Decision Support to Minimize Further Harm
https://www.cisa.gov/sites/default/files/publications/CISA_Insight_Provide_Medical_Care_Sep2021.pdf.
[60] CDC MMWR Impact of Hospital Strain on Excess Deaths During the COVID-19 Pandemic — United States, July 2020–July 2021 https://www.cdc.gov/mmwr/volumes/70/wr/mm7046a5.htm.
[61] CISA COVID Task Force: "Provide Medical Care is in Critical Condition" December 2021
https://www.youtube.com/watch?v=F-uh-lx_KKU&t=6s.
[62] WSJ Hospital Hit by Hackers, a Baby in Distress: The Case of the First Alleged Ransomware Death
https://www.wsj.com/articles/ransomware-hackers-hospital-first-alleged-death-11633008116.
[63] Entering uncharted territory, the U.S. counts 500,000 Covid-related deaths.
https://www.nytimes.com/2021/02/22/us/us-covid-deaths-half-a-million.html.
[64] Delays in Emergency Care and Mortality during Major U.S. Marathons
https://www.nejm.org/doi/full/10.1056/nejmsa1614073.

FIGURE. Estimated number of excess deaths* 2 weeks after corresponding percentage of adult intensive care unit bed occupancy — United States, July 2020–July 2021



* Upper and lower boundaries of shaded area indicate 95% CIs.

Cybersecurity & Infrastructure Security Agency, unpublished data, 2021). As hospitals exceed 100% ICU bed capacity, 80,000 (95% CI = 53,576–132,765) excess deaths would be health care and public health sectors, with excess deaths emerging in the weeks after a surge in COVID-19 hospitalizations. The results of this study support a larger body of evidence

While this Excess Death math is a feature of the pandemic strains, the systems analysis revealed the elevated risk of loss of life when (for example) ambulance diversions are too far away for the time-sensitive conditions. Also, with the financial strains from covid and the substantive losses of skill workers in healthcare, we will not return to safer capacity levels for some time.

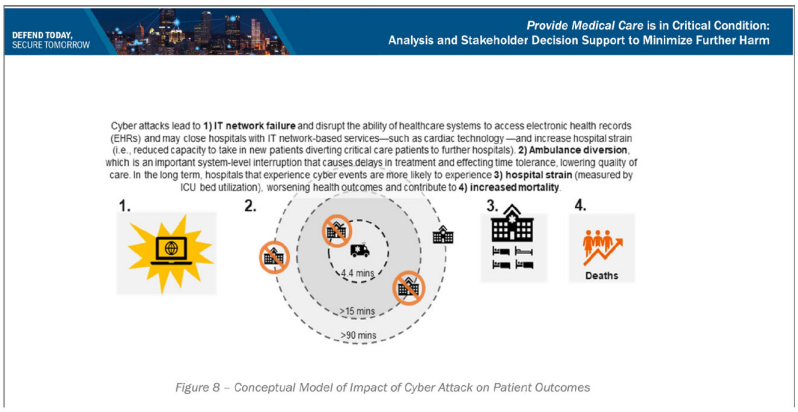


Figure 8 – Conceptual Model of Impact of Cyber Attack on Patient Outcomes

Pragmatism for the Target Rich; Cyber Poor:
Years ago, my colleague from industry, Wendy Nather coined: "Living Below the Security Poverty Line."[65] Throughout my emergency Federal Service, and with a focus on Critical Infrastructure, I channeled this into what I've been calling **Target Rich; Cyber Poor.** An entity can be **Cyber Poor** if there is a deficiency in one or more of the following three areas:

- Insufficient Information/Awareness
- Insufficient Incentives (Carrots/Sticks)
- Insufficient Resources

Going back to the 405c Task Force Report, **our estimate was that 85% of the healthcare delivery organizations in the country lack a single, experienced cybersecurity person on staff**. We saw similarly prone targets in the vaccine supply chain ball bearings. We saw similar conditions in Water & Waste Water, in Food Production, etc.

There is a massive split between the *Haves* and the *HaveNots* of critical infrastructure. The *Haves* might attempt "Best Practices" and are likely in or around Sector Coordinating Councils and ISACS and running the race. The *HaveNots* of the Cyber Poor may not even be at the starting line. It became clear to me that we would need to reckon with these *HaveNots* - meet them where they are, and identify and buy down risk… *Crawl, then Walk, then Run.*

[65] Security Ledger Episode 223: CISA Looks To Erase The Security Poverty Line https://securityledger.com/2021/08/episode-223-cisa-looks-to-erase-the-security-poverty-line/.

During the Microsoft Exchange attacks,[66] I watched the Cyber Poor / Resource Poor being encouraged to "Implement Zero Trust" or "Just Do Best Practices". Many were asking if software updates would be provided for their Unsupported versions of Exchange. The Chief Data Scientist of Rapid7, Bob Rudis, then surveyed the Internet to find that the dominant versions of Exchange were unsupported. This was especially bad in healthcare. I decided that day that we needed to invert the script. I started working on CISA's "**Bad Practices**" - the most dangerous practices for owners and operators of critical infrastructure.[67] This list currently has three entries including: the first of which, the use of Unsupported and End of Life Software in service of Critical Infrastructure.

Next I shifted to something I teach my CMU students: **S.O.S.** Get your "stuff" off search.[68] See what your adversaries see about your internet facing infrastructure. We wrote CISA's *Stuff Off Search* program. A free way to see if your assets are showing - and how to reduce that attack surface.

We use **S.O.S.** as a gateway to the free, taxpayer funded CISA **Cyber Hygiene (CyHy)** Scanning Service – which will send daily scan results of known vulnerabilities to you.[69] And since you likely cannot fix all of them, the CISA **KEV** list can tell you the **K**nown **E**xploited **V**ulnerabilities to prioritize first.[70]

Since attacks are likely to be successful, perhaps the best way to know how you might fare is to practice failure with lightweight **table top crisis simulations** (also offered by CISA).[71]

We rolled these together into a collection we informally called the *Pragmatic Security Suite*… a short set of self service webinar videos.[72]

Be under no illusions… these will not make the Cyber Poor immune to attackers. But they may be the difference in opportunistic attacks. This starts their journey… but there will need to be strong incentives and assistance to advance this journey.

Good steps - in need of acceleration:
There are some bright spots, but these efforts need to move more quickly.

---

[66] The Microsoft Exchange Server hack: A timeline https://www.csoonline.com/article/3616699/the-microsoft-exchange-server-hack-a-timeline.html.
[67] CISA Bad Practices https://www.cisa.gov/BadPractices.
[68] CISA Stuff Off Search https://www.cisa.gov/publication/stuff-off-search.
[69] CISA Cyber Hygiene Services https://www.cisa.gov/cyber-hygiene-services.
[70] CISA Known Exploited Vulnerabilities Catalog https://www.cisa.gov/known-exploited-vulnerabilities-catalog.
[71] CISA Tabletop Exercises Packages https://www.cisa.gov/cisa-tabletop-exercises-packages.
[72] The Pragmatic Cyber Security Series https://www.cisa.gov/pragmatic-cyber-security-webinar.

- The FDA CyberSecurity Pre-Market[73] and Post-Market[74] Guidance: Suzanne Schwartz has leaned-in and shown bold leadership. She needs more support and authority to drive these advances more quickly.[75,76] Hospitals are desperate for these fortifications. This is helpful for FDA approved technologies, but EHRs and other non-FDA regulated. healthcare tech require similar levels of care
- SBOM[77] (Software Bill of Materials): This Software Supply Chain foundational enabling artifact/practice is in the FDA Pre-Market Draft,[78] enjoyed an 3.5 voluntary cultivation via NTIA,[79,80] made it into President Biden's CyberSecurity Executive Order,[8182] and is *increasingly* proving its necessity on large scale issues like the most recent Log4j exposures.[83,84] Parts of industry still fear this transparency and want to go more slowly than we can afford. The Healthcare Proof of Concept team developed an open source tool "Daggerboard" to ingest/manage SBOMs to protect hospitals… its full value will grow as SBOMs become more readily available
- Medical/Clinical Hacking Simulations: I am The Cavalry teamed with doctors to start the Cyber Med Summits[85,86,87] - now a formal 501(c)(3) non-profit. ER & OR hacking simulations and table-top exercises show healthcare stakeholders how real medical technology hacks affect patient care. We have hacked insulin

---

[73] Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions Draft Guidance for Industry and Food and Drug Administration Staff https://www.fda.gov/media/119933/download.
[74] Postmarket Management of Cybersecurity in Medical Devices https://www.fda.gov/regulatory-information/search-fda-guidance-documents/postmarket-management-cybersecurity-medical-devices.
[75] H.R.7084 - PATCH Act of 2022 https://www.congress.gov/bill/117th-congress/house-bill/7084/text
[76] S.3983 - PATCH Act https://www.congress.gov/bill/117th-congress/senate-bill/3983/text
[77] NTIA Software Bill of Materials https://www.ntia.gov/sbom.
[78] 115th Congress of the United States Committee on Energy and Commerce Letter from Chairman Walden to Acting Secretary Hargan https://republicans-energycommerce.house.gov/wp-content/uploads/2017/11/20171116HHS.pdf.
[79] NTIA Launches Initiative to Improve Software Component Transparency https://www.ntia.doc.gov/blog/2018/ntia-launches-initiative-improve-software-component-transparency
[80] NTIA Software Component Transparency https://www.ntia.gov/SoftwareTransparency.
[81] EO 14028: Improving the Nation's Cybersecurity https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity.
[82] EO 14028: The Minimum Elements For a Software Bill of Materials (SBOM) https://www.ntia.doc.gov/report/2021/minimum-elements-software-bill-materials-sbom.
[83] Log4j is why you need an SBoM https://blog.reversinglabs.com/blog/log4j-is-why-you-need-an-sbom.
[84] Nature: Building resilient medical technology supply chains with a software bill of materials https://www.nature.com/articles/s41746-021-00403-w.
[85] CyberMed Summit https://www.cybermedsummit.org/.
[86] ABC Nightline: Fears of hackers targeting US hospitals, medical devices for cyber attacks https://abcnews.go.com/Health/fears-hackers-targeting-us-hospitals-medical-devices-cyber/story?id=48348384.
[87] Mark Albert: Efforts to protect patients from cyberattacks grow https://www.wisn.com/article/efforts-to-protect-patients-from-cyberattacks-grow/27493371#.

pumps, pacemaker defibrillators,[88,89] bedside infusion pumps, imaging systems, blood bank databases, building automation systems, EHRs, and more. Experiential learning forums like these could inform and inspire more awareness - sooner.

- Mandatory Breach Reporting[90] to CISA: I was pleased to see this passed into law, but disappointed to see a multi-year rule making process. With so many attacks and such poor reporting, we need to move as quickly as possible. We cannot shift to studying and preventing attacks without adequate and timely visibility into them
- Bad Practices[91] are declared: Who will help to drive them toward extinction? Sector Specific Regulators? FTC? SEC? The Insurance Industry is talking about their role… I could see arguments around due care and negligence getting traction if encouraged
- SRMAs (Sector Risk Management Agencies) are now in statute: but/and the interagency, shared responsibility model with CISA (and FBI, etc) is *far* from where it needs to be. Our CISA Covid Task Force got a lot of great things accomplished outside of interagency comfort zones… and I fear those positive models have diminished since our task force was ended. **Cybersecurity is a team sport**… the sooner we find the optimal shared responsibility model… the sooner we can do what the country needs us to… Perhaps the newly formed ONCD in the White House can assist here

Failed Markets & Getting Beyond Voluntary:
Congress has acted in directionally-correct ways - plural times.[92,93] Industry prefers voluntary… and yet, we're now seeing more and more devastating attacks to healthcare.[94,95,96] Critical Infrastructure needs to work.

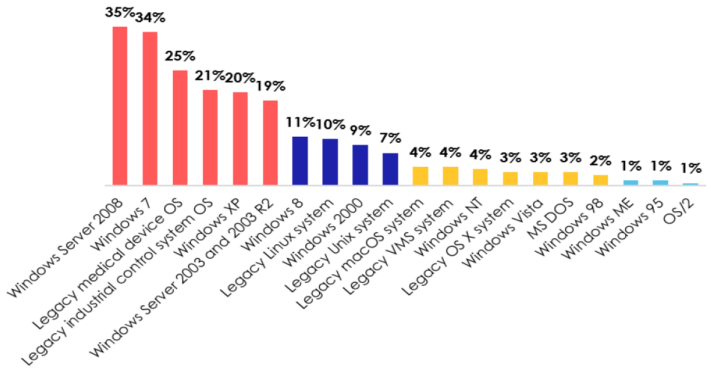
The NIST CYbersecurity Framework is voluntary - and nearly a decade later, OIG reports show we still have poor visibility into if it is being used or not.[97] The

---

[88] Digital Defenses for Hacked Hearts: Why Software Patching Can Save Lives
https://www.jacc.org/doi/10.1016/j.jacc.2018.03.540
[89] FDA Warning Letter - Abbott (St Jude Medical Inc.)
https://www.fda.gov/inspections-compliance-enforcement-and-criminal-investigations/warning-letters/abbott-st-jude-medical-inc-519686-04122017
[90] H.R.2471 - Consolidated Appropriations Act, 2022
https://www.congress.gov/bill/117th-congress/house-bill/2471/text
[91] CISA Bad Practices https://www.cisa.gov/BadPractices.
[92] 115th Congress of the United States Committee on Energy and Commerce Letter from Chairman Walden to Acting Secretary Hargan
https://republicans-energycommerce.house.gov/wp-content/uploads/2017/11/20171116HHS.pdf
[93] H.R.4611 - DHS Software Supply Chain Risk Management Act of 2021
https://www.congress.gov/bill/117th-congress/house-bill/4611/text.
[94] RTF Report: Combating Ransomware - A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force
https://securityandtechnology.org/ransomwaretaskforce/report/.
[95] Nine security lessons from the 'Conti cyber attack on the HSE' report
https://bhconsulting.ie/nine-security-lessons-from-the-conti-cyber-attack-on-the-hse-report/.
[96] Mark Albert: Efforts to protect patients from cyberattacks grow
https://www.wisn.com/article/efforts-to-protect-patients-from-cyberattacks-grow/27493371#.

Cybersecurity Act of 2015 reduced the risk of information sharing and provided some safe harbor for reporting to CISA, yet it isn't being used for more than a tiny fraction of publicly observable attacks. FDA has done a great job raising the bar for the Cybersecurity of new devices and have even issued safety communications and affected recalls.[98,99] Yet hospitals continue to use these recalled devices and unsupported devices - as the norm. Without HHS CMS and/or Joint Commission requirements, we will remain prone. And… With mandatory minimums, there may need to be assistance. Our 405c Task Force had suggestions for Cash-For-Clunkers-like models for technology refresh programs to remove the most dangerous equipment from rotation. HIMSS surveys show legacy & unsupported software remains unaddressed[100]

Figure 12: Legacy (Unsupported) Operating Systems in Place



Seatbelts weren't voluntary. I don't believe fire escapes were voluntary - nor kitchen sanitation codes for commercial restaurants. Public Safety isn't free. The lack of sufficient public safety and public good is also dis-economic. Further crisis of confidence in the public in modern healthcare will drive devastating harms to the public safety, economic, and national security.

---

[97] Medicare Lacks Consistent Oversight of Cybersecurity for Networked Medical Devices in Hospitals https://oig.hhs.gov/oei/reports/OEI-01-20-00220.asp.

[98] LifeCare PCA3 and PCA5 Infusion Pump Systems by Hospira: FDA Safety Communication - Security Vulnerabilities https://wayback.archive-it.org/7993/20170112164109/http:/www.fda.gov/Safety/MedWatch/SafetyInformation/SafetyAlertsforHumanMedicalProducts/ucm446828.htm.

[99] FDA warns of security flaw in Hospira infusion pumps https://www.reuters.com/article/hospira-fda-cybersecurity-idCNL1N10B2GY20150731.

[100] 2021 HIMSS Healthcare Cybersecurity Survey Report https://www.himss.org/resources/himss-healthcare-cybersecurity-survey.

The Therac-25 radiation delivery machine's software design flaws killed people.[101,102] At the time, they wanted to give it a few more years before we introduced liability to software.[103,104] That was 37 years ago. We're now seeing more brazen adversaries, more nation state use of cyberwarfare, and more frequent and consequential attacks on designated critical infrastructure.

As the world is increasingly depending upon digital infrastructure,[105] that infrastructure needs to be more dependable.

The cybersecurity of healthcare is not trending in the right direction. We can do something about that. We must.

---

[101] An investigation of the Therac-25 accidents https://ieeexplore.ieee.org/document/274940.
[102] The Therac-25: 30 Years Later https://www.computer.org/csdl/magazine/co/2017/11/mco2017110008/13rRUxAStVR.
[103] 2014 RSAC Webinar - Software Liability?: The Worst Possible Idea (Except for all Others) https://www.rsaconference.com/library/webcast/webcast-software-liability-the-worst-possible-idea-except-for-all-others.
[104] 2017 RSAC Talk: SW Liability? Uncomfortable Truths Require Uncomfortable Response https://youtu.be/yGlAC6zxVnc.
[105] Andrea Matwyshyn - Internet of Bodies https://scholarship.law.wm.edu/wmlr/vol61/iss1/3/.

[SUMMARY STATEMENT OF JOSHUA CORMAN]

Attacks on healthcare are increasing in volume, variety, and impact—with consequences now including the loss of life. While directionally correct steps have been taken, we're getting worse faster than we're getting better. Bold actions and assistance will be required to change this trajectory, address these market failures, lack of incentives, and historical under-investments.

Attackers have gotten stronger, but defenders have not—and many got weaker. The number of healthcare attacks have grown. The costs of the ransom payments have grown. [1] The impact of attacks are no longer merely measured by record count, fines, ransom payments, or recovery costs . . . but include double-digit millions of lost revenue and worse . . . **degraded patient care and human life**. [2] Hurried crisis adjustments added more technologies and attack surfaces. Financial constraints forced reduced investments in cybersecurity staff & operating budgets.

"**Cyber Safety is Patient Safety**". I love my privacy; I'd like to be alive to enjoy it. Defensible connected technologies will require investment—as will the talent to defend them. Scrubbing-in before surgery takes time/money—and this vital hygiene practice dramatically reduces post-op infection, complications, and mortality rates. As technology increasingly plays a role in the delivery of modern healthcare, cyber-hygiene is no longer negotiable. Many exclaim they can't afford to do more. I hear Stan Lee: *With Great Connectivity, Comes Great Responsibility . . .*

The pandemic brought an untenable, perfect storm of a record high need for patient care in the face of record high adversary activity, and severely diminished resources with which to defend the healthcare delivery environments. [3]

Degraded and delayed care affects patient outcomes. Cybersecurity disruptions can cause and exacerbate delays and degrade care for a hospital, town, region, or even at the state level. Adversaries are disrupting the bottom of Maslow's Hierarchy of Needs. Insecurity at the base of his famous pyramid is not tenable for an individual—and certainly not sustainable for a country. Do not mess with Maslow . . .

Last, purely voluntary efforts have not proven able to transcend these market failures-and we're on a troubling trajectory with increasingly aggressive nationstates attacks. We have useful building blocks, but they require more speed & support. As the world is increasingly depending upon digital infrastructure, that infrastructure needs to be more dependable.

The CHAIR. Thank you.

Ms. McLaughlin.

STATEMENT OF AMY MCLAUGHLIN, CYBERSECURITY PROGRAM DIRECTOR, CONSORTIUM OF SCHOOL NETWORKING, CORVALLIS, OR

Ms. MCLAUGHLIN. Chair Murray, Senator Cassidy, and Members of the Committee, it is an honor to be here with you today to talk about the cybersecurity threats and challenges facing K–12 education. As mentioned earlier, I am Amy McLaughlin. I maintain multiple cybersecurity certifications and have over 20 years' experience as a cybersecurity professional that spans state and local Government, K–12 and higher education, and health care.

I serve as the Cybersecurity Program Director for the Consortium of School Networking, CoSN, the national organization dedicated to meeting the needs of K–12 education technology leaders. K–12 school districts face increasing attacks and threats. Today's cyber threats largely come from organized crime, nation state actors, and terrorist organizations.

---

[1] RTF Report: Combating Ransomware *https://securityandtechnology.org/ransomwaretaskforce/report/*.

[2] CISAInsights Provide MedicalCare is in CriticalCondition https://www.cisa.gov/sites/default/files/publications/CISA-Insight-Provide-Medical-Care-Sep2021.pdf.

[3] Ransomware Hits Dozens of Hospitals in an Unprecedented Wave *https://www.wired.com/story/ransomware-hospitals-ryuk-trickbot/*.

The most prevalent threats facing K–12 schools are ransomware attacks designed to encrypt and block data access to computer systems until a ransom is paid, phishing attacks that inundate education employees with fraudulent emails, attempting to trick them into responding with sensitive data, distributed denial of service attacks that flood the target networks making them inaccessible, and cybersecurity—or cyber-attacks against vendors providing services to multiple districts that result in wide scale impacts.

The impacts of cyber-attacks on K–12 school districts, teachers, and students include lost instructional time, damage to schools' reputations, high financial costs of cyber incidents, rising cybersecurity insurance costs, financial and credit hardships for students and employees from the loss of their personal data, and rising mental health impacts, including increases in anxiety and depression.

These impacts are being realized around the country. In Toledo, Ohio, and Fairfax County, Virginia, attackers threatened to make personal information of students and educators public. School districts in Baltimore, Maryland and Hartford, Connecticut were forced to shut down and cancel several days of school due to ransomware. And on the first day of classes, the Miami-Dade County Public Schools in Florida, the fourth largest U.S. district, saw their networks overwhelmed by denial of service attack.

K–12 schools and districts experience significant challenges in protecting themselves from cyber-attacks. Most districts see cybersecurity as a technical issue, and it isn't. It is an issue that requires everybody in an organization to understand and be part of the solution and understand their role in protecting the organization. Safeguarding technologies are expensive, and the leading K–12 funder, the E-Rate program, does not fund cybersecurity or network defenses.

School districts struggle to hire cybersecurity professionals. With almost 500,000 unfilled positions in cybersecurity in the United States, districts cannot compete with private sector salaries and opportunities. Digital equity is a significant challenge as cyber issues, security issues disproportionately impact our school districts who have less funding available to support and secure their technologies.

The addition of Internet of Things devices to networks demand additional protections the districts are unable to fund and unprepared to deliver. Our K–12 school systems are taking many steps already to improve and expand protections for data and IT systems, including training their IT staff in cybersecurity, training their end users to protect themselves from cyber-attack, backing up data to offsite facilities to recover faster from ransomware attacks, and upgrading their password requirements from basic eight character passwords to stronger pass phrases and implementing multiple factor authentication.

But there are additional Federal actions that should be taken to help our schools and districts improve their cybersecurity defenses. E-Rate needs to be updated to include cybersecurity and expand the E-Rate definition of firewalls to encompass next generation firewalls and services.

We need to encourage the U.S. Department of Education through the Privacy Technical Assistance Center to expand guidance materials and coordinate services across Federal agencies. We need support for implementation of Representative Matsui's 2021 Enhancing K–12 Cybersecurity Act, which CoSN has endorsed.

We need funding, additional funding for MS-ISAC to provide their fee based services to K–12 free of charge. Additionally, funding university and college run security operations centers, or SOCs, which offer cost effective services for K–12 schools and train new cybersecurity professionals, is an excellent opportunity, and we need to help schools hire expert staffing.

Our K–12 districts are on the front lines of protecting their data and systems against much larger, better funded organizations and a rapidly evolving cyberthreat environment. They need access to staffing and technical resources and continue to securely deliver education. I thank you for your time and look forward to your questions.

[The prepared statement of Ms. McLaughlin follows:]

PREPARED STATEMENT OF AMY MCLAUGHLIN

Chair Murray, Ranking Member Burr and Members of the Committee:

It is an honor to be with you today to talk about the cybersecurity threats and challenges facing K-12 education. I'm Amy McLaughlin, I maintain multiple cybersecurity certifications including the Certified Information Systems Security Professional (CISSP), and Certified Information Systems Manager (CISM). I have over 20 years of experience as a cybersecurity professional that spans state and local government, K-12 and higher education, and health care. I serve as the Cybersecurity Program Director for the Consortium of School Networking (CoSN) the national organization dedicated to meeting the needs of K-12 education technology leaders.

These challenges were daunting before the COVID–19 pandemic, and the rapid deployment of millions of one-to-one mobile devices to shift schools to remote and hybrid learning expanded the technology footprint and increased opportunities for malicious attacks.

The threats faced by K 12 schools and the education sector are very serious and constantly changing. Gone are the days where cyber threats came from individual "script kiddies" who sought to access systems, write viruses and worms just to see if they could. Today's cyber threats come from organized crime, nation state actors, and terrorist organizations[1] who have three objectives—use cybercrime to make money through ransoming data or stealing and selling data, collecting data for future use, and disrupting U.S. infrastructure and daily life with attacks on our ability to offer a free public education. In addition to external threats, education faces internal threats from students who can quickly and easily learn how to buy or conduct disruptive attacks online.

Attacks against the K-12 system are increasing. In December 2020, the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and the Multi-State Information Sharing and Analysis Center (MS-ISAC) issued a TLP:WHITE level Joint Advisory[2] identifying K-12 as targets of opportunity for cyber actors and identified increased attacks against education organizations.

The increase in attacks is reflected in the data around ransomware attacks. The 2020 Joint Advisory cited the MS-ISAC data indicating that "the percentage of reported ransomware incidents against K–12 schools increased at the beginning of the 2020 school year. In August and September, 57 percent of ransomware incidents reported to the MS-ISAC involved K–12 schools, compared to 28 percent of all reported ransomware incidents from January through July." This trend continued into 2021 and continues to be a significant issue going into 2022. Bad actors do not dis-

[1] *https://www.cisa.gov/uscert/ics/content/cyber-threat-source-descriptions.*
[2] *https://www.cisa.gov/uscert/ncas/alerts/aa20-345a.*

criminate by location. Cyberattacks hit the biggest urban and suburban school districts as well as the smallest rural schools.

Our K-12 schools and districts recognize the serious privacy, monetary, and operational significance of the cyber threats. CoSN's 2022 Ed Tech Trends report identified cybersecurity as the top unmet technology need stating that even before the pandemic required schools to move more services online, cybersecurity has been a top concern for districts. In a situation where even well-funded corporations in the private sector struggle to address cybersecurity issues, poorly funded districts are at a disadvantage. One respondent called the need for more cybersecurity funding as "desperate."

Cybersecurity is not only an unmet technology need; it is an organizational culture challenge. K-12 organizations are vulnerable to cyber actors who leverage phishing attacks and social engineering skills to attack school systems with ransomware and other malware or obtain login credentials to access and hack systems. These attacks exploit the helpful and service-oriented focus of school staff and teachers to perpetrate malicious attacks. School district technology leaders work to help staff and teachers recognize these tricks but cybersecurity education must become a more systemic part of educator preparation and professional development and other staff training.

There are many cybersecurity threats facing K–12 schools. In lieu of providing an exhaustive list, I'll share with you the most prevalent threats:

Ransomware and other malware attacks are often the most destructive and disruptive threat facing education. Ransomware is malicious software designed to encrypt files and block access to computer systems until a sum of money is paid. The more advanced forms of ransomware not only encrypt files, they also exfiltrate the files to the attacker who can then hold the data hostage, resell the data on the dark web, or collect the data for later uses that are, as yet, unknown and, in the case of data stolen by nation state actors, may become a national security threat. Just to be clear, these bad actors are stealing the most damaging and sensitive student, family, employee, and district financial data held by school districts and disseminating it to the highest bidder.

The State of Louisiana experienced the devastating impact of ransomware in 2019 when Louisiana's Governor had to declare a state of emergency after a series of cyber-attacks shut down phones and locked and encrypted data at three of the state's school districts.[3] The attack disrupted teaching and learning and ransomware response ultimately cost the state over $2.3 million.[4] 75,000 students in Albuquerque, NM missed 2 days of school in a 2022 ransomware attack.[5]

Second, education is inundated with ongoing phishing attacks through school district and other email systems. Phishing is an attack that leverages sending fraudulent emails purporting to be from reputable companies and organizations in order to trick individuals to reveal personal information, such as passwords and credit card numbers or send data directly to the cyber actor for example, W2 forms and gift card numbers. "Phishing attacks are responsible for more than 80 percent of reported security incidents. According to CISCO's 2021 Cybersecurity Threat Trends report, about 90 percent of data breaches occur due to phishing. Spear phishing is the most common type of phishing attack, comprising 65 percent of all phishing attacks. The 2021 Tessian research revealed that employees receive an average of 14 malicious emails every year".[6]

Third, schools are frequently victims of (DDOS) distributed denial of service attacks. DDOS attacks occur when multiple machines are operating together to attack one target, they flood the target network, server or system, with traffic and illegitimate activity disabling the systems and making them inaccessible. As the FBI, CISA, MS-ISAC Joint Advisory noted, the availability of DDoS-for-hire services provides opportunities for any motivated malicious cyber actor to conduct disruptive attacks regardless of experience level, including students. Miami-Dade School District experienced a particularly disruptive DDoS attack in September 2020 that impacted the districts ability to offer 200,000 students remote learning for the first 2 days

---

[3] *https://www.cnbc.com/2019/07/26/louisiana-declares-state-of-emergency-after-cybercriminals-attack-school-districts.html.*

[4] *https://www.theadvocate.com/baton—rouge/news/politics/legislature/article-caf129ae-5e62-11ea-912b-77e0d8405441.html.*

[5] *https://www.usnews.com/news/best-states/new-mexico/articles/2022-01-18/albuquerque-schools-confirm-ransomware-attack-resume-class.*

[6] *https://spanning.com/blog/cyberattacks-2021-phishing-ransomware-data-breach-statistics/.*

of the school year.[7] This attack was perpetrated by a 16-year old high school junior.[8]

A less obvious, but large threat to K-12 schools, are cyber-attacks against third party companies that provide essential operational and instructional technologies . Many K-12 school systems leverage software as a service providers and cloud hosted systems to deliver important technologies for supporting teaching, learning and the delivery of school services including student information systems, learning management systems, ERP systems for finance and human resources, and more. Attacks against third party services providers can result in wide scale outages for schools and widescale data theft or data destruction. Examples of vulnerable and exploited third-party tools that have impacted K-12 education include the 2020 SolarWinds hack,[9] the 2021 Log4J vulnerability that had organizations scrambling to identify vulnerable systems and remediate them,[10] and the 2022 data breach at Illuminate Education which impacted at least 24 districts.[11]

Additional threats include social engineering, end of life and unsupported software and operating systems, open and exposed Internet of Things (IoT) systems, video conference disruptions, website defacement and hacktivism, and more.

The impacts of cyberattacks on K-12 school systems are extensive. Students are directly impacted by lost instructional time when schools are closed as a result of ransomware or other debilitating attacks. Successful cyberattacks damage the reputation of schools and undermine trust of students and parents in the ability of school districts to protect student data and maintain consistent services. Cyberattacks are a crime, yet school districts who are victimized by these sophisticated criminal operations face blame for the crime.

The cost of responding to a cybersecurity incident, restoring systems, and providing services to impacted students and staff is high. In 2021, the average data breach by in the education sector costs $3.79 million.[12] The cost per individual record lost to a data breach can exceed $165 per record. These costs roll over to other schools and districts as insurance companies raise cybersecurity premiums and deductibles. Cybersecurity insurance costs for K-12 are rising by 25–300 percent with more limited coverage and high deductible.[13]

School districts across the country are facing rising insurance costs regardless of whether they have had a cybersecurity incident or not. Not only are insurance premiums increasing, the ability to even become insured has now become predicated on successful completion of a risk assessment and implementation of specific cybersecurity safeguards. The costs of new cybersecurity safeguards and rising insurance premiums prices many school districts out of the insurance market.

There are individual financial and psychological impacts to staff and student victims of cybersecurity attacks. Individuals whose identities are stolen face financial hardship from the loss of their personal data, and students whose identities are stolen may not realize the full financial impact until much later. Since 2017 there has been a growing trend of sales of student data on the dark web. Identities of students who are too young to have existing credit accounts are valuable commodities.

Students under 18, without existing credit accounts, have found themselves victims of identity theft and credit card fraud when stolen data is used to open accounts using their information. Often the fraudulent accounts go undetected until students apply for financial aid for college, or attempt to obtain credit for the first time only to discover their credit is destroyed and their finances are crippled by data theft from a previous cyber-attack.

---

[7] *https://thehill.com/policy/cybersecurity/514802-miami-dade-school-district-virtual-classes-disrupted-by-cyberattack/*.

[8] *https://www.nytimes.com/2020/09/03/us/miami-dade-school-cyberattack.html*.

[9] *https://www.zdnet.com/article/sec-filings-solarwinds-says18000-customers-are-impacted-by-recent-hack/*.

[10] *https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance*.

[11] *https://thejournal.com/articles/2022/05/03/illuminate-education-data-breach-impacted-at-least-24-districts-18-charter-schools-in-ny.aspx*.

[12] Cost of a Data Breach Report 2021, IBM Security https://doc-0k-5g-apps-viewer.googleusercontent.com/viewer/secure/pdf/pp9sepf14apgmvrtn4gr78ef7erikjgp/ke3i7gc3usr03dhfesplfnjgpfsrg4d1/1652374200000/drive/14468447276760910654/ACFrOgDH7U4d-azWxsI9zUMG-du0g1d1xPAzRyNRZOZ80u9mK7921h7ZxHLm0C2HHrjSTa-LsSLDcpD-iREpwtCR4j-9Y6RT8Kdpooo7pTum8mhiQ9IZ0kRnnJtex2inBASkqwbNCRUozGq4Vg1B?print=true.

[13] *https://www.businessinsurance.com/article/20220216/NEWS06/912347780/Perspectives-New-lessons-for-K-12-schools-on-cyber-security,-insurance-cover-#:~:text=K—2D12—20schools—20face—20a,deductibles—20and—20narrower—20coverage—20terms*.

Data breaches and identity theft also result in mental health impacts. According to a recent survey by the nonprofit Identity Theft Resource Center, "86 percent of identity theft, victims reported feeling worried, angry and frustrated, nearly 70 percent felt they could not trust others and felt unsafe, and nearly 85 percent reported disturbances in their sleep habits and 77 percent reported increased stress levels, and nearly 64 percent, they had trouble had trouble concentrating."

K–12 schools and districts experience significant challenges in protecting themselves from cyberattack. First, school districts are not funded to purchase in depth cybersecurity technologies to safeguard their systems and data. These technologies are expensive and existing mechanisms funding high speed internet access, such as the E-rate program, do not fund network defenses.

Staffing and the ability to hire cybersecurity professionals is another challenge school districts face. There are not enough cybersecurity professionals available and school districts can't afford them. According to , "Only a fifth (21 percent) of districts have a full-time equivalent (FTE) employee dedicated to network security, the same percentage as the prior year. This means that cybersecurity protection is a part-time responsibility in a large majority of school districts . . . In lieu of a full-time cybersecurity position, districts address cybersecurity in a variety of ways. A third (33 percent) of districts include the responsibility as part of another job."

Today there are almost 500,000 unfilled cybersecurity positions in the United States that number is projected to increase. School districts struggle to find qualified cybersecurity staff who will work for a K–12 salary. The competition for skilled cybersecurity professionals also results in districts making tough choices between hiring one or two teachers or hiring a cybersecurity professional.

Ensuring cybersecurity equity in education is a significant challenge. Every school district faces cybersecurity threats, but they disproportionately impact school districts with less funding available to staff, support, and secure their technologies. Often, rural, and low-income schools and districts have less funding available to hire dedicated expert staff and maintain their technology up-to-date resulting in higher risk of unsupported and aging systems vulnerable to attack.

Recognizing the many attack vectors and challenges they face, K–12 school systems are taking many steps to improve and expand protections for data and IT systems. The 2022 CoSN Ed Tech Leadership Survey identified the following steps being taken to protect data and systems:

- 65 percent of schools and districts responding to the survey focusing on IT staff training to help grow the skills of their staff in the cybersecurity space. In lieu of hiring trained cybersecurity professionals, districts are seeking to grow these skills internally.
- 63 percent are investing in end-user training which can address the
- 55 percent are leveraging offsite backups which is the No. 1 step districts can take to be able to recover quickly from a ransomware attack.
- 54 percent were working with staff to upgrade their passwords to expand from a basic eight-character password to a stronger passphrase of at least 12 characters. Increasing the number of characters in a password from eight to 12 characters increases the time a supercomputer needs to brute-force crack a password from minutes to centuries. [14]

There are additional steps that can be taken at a national level to help schools and districts improve cybersecurity defenses and services across the country.

(1) Update E-rate's definition of firewall to encompass next-generation firewalls and services. CoSN [15] filed a petition with the Federal Communications Commission in 2021 requesting this change. This does not require legislation and the FCC can and should immediately take this action.

(2) Encourage the U.S. Department of Education through the Privacy Technical Assistance Center to expand guidance materials and coordinate services across Federal agencies to provide a comprehensive menu of products.

(3) Support the implementation of Rep. Matsui's 2021 Enhancing K–12 Cybersecurity Act, [16] which CoSN has endorsed.

---

[14] Firewalls Don't Stop Dragons, Fourth Edition, Cary Parker, Apress, p.109.

[15] *http://d31hzlhk6di2h5.cloudfront.net/20190903/cc/f3/72/41/228e09116606c764f2d2f2c4/CoSN-Cat-Two-Filing-Final-2019. pdf.*

[16] *https://www.Congress.gov/bill/117th-congress/house-bill/4005-q=—7B—22search—22—3A—5B—22hr-3—22—5D—7D&s=1&r=64.*

(4) Fund MS-ISAC to provide their fee-based services to K-12 free of charge and expand staffing of their Security Operations Center.

(5) Fund university and college run Security Operations Centers (SOCs). Colleges and universities are developing non-profit SOCs offer cost-effective services for K-12 schools and train new cybersecurity professionals increasing the number of people capable of filling open positions.

(6) Help schools hire expert staffing.

Our K-12 school districts are on the front lines of protecting their data and systems against much larger, better funded organizations, and a rapidly evolving cyber threat environment. To borrow a quote from "Hamilton" they are "outgunned, outmanned, outnumbered, out planned." They need access to staffing and technical resources to continue to securely deliver on the mission of delivering education.

[SUMMARY STATEMENT OF AMY MCLAUGHLIN]

K-12 school districts face increasing attack and threats. Today's cyber threats largely come from organized crime, nation state actors, and terrorist organizations.

The most prevalent threats facing K-12 schools are:

- **Ransomware** attacks designed to encrypt files and block access to computer systems until a sum of money is paid are increasing.
- **Phishing** attacks that inundate education employees with fraudulent emails attempting to trick them into responding with sensitive data.
- **Distributed denial of service attacks** (DDOS) that flood the target networks making them inaccessible.
- **Cyber-attacks against vendors** providing services to multiple districts with widescale impacts

The impacts of cyberattacks on K-12 school districts, teachers and students include:

- Lost instructional time
- Damage to schools reputations
- Financial costs of cyber incidents
- Rising cybersecurity insurance costs
- Financial and credit hardships for students and employees from the loss of their personal data
- Mental health impacts including anxiety and depression

K–12 schools and districts experience significant challenges in protecting themselves from cyberattack

- Safeguarding technologies are expensive and the leading K-12 technology funder—the E-rate program—does not fund network defenses
- School districts struggle to hire cybersecurity professionals. With almost 500,000 unfilled cybersecurity positions in the United States, districts can't compete with private sector salaries
- Digital equity is a significant challenge as cybersecurity issues disproportionately impact school districts with less funding available to support and secure their technologies
- The addition of Internet of Things (IoT) devices to networks demand additional protections

Our K–12 school systems are taking many steps to improve and expand protections for data and IT systems including:

- Training IT staff training in cybersecurity
- Training end-users to protect themselves from cyber attacks
- Backing up data to offsite locations to facilitate faster recovery from a ransomware attack
- Upgrading password requirements from a basic eight-character password to a stronger passphrase of at least 12 characters and implementing multi-factor authentication

There are additional Federal actions that should be taken to help schools and districts improve cybersecurity defenses:

(1) Update E-rate's definition of firewall to encompass next-generation firewalls and services.

(2) Encourage the U.S. Department of Education through the Privacy Technical Assistance Center to expand guidance materials and coordinate services across Federal agencies.

(3) Support implementation of Rep. Matsui's 2021 Enhancing K–12 Cybersecurity Act, which CoSN has endorsed.

(4) Fund MS-ISAC to provide their fee-based services to K–12 free of charge and expand staffing of their Security Operations Center.

(5) Fund university and college run Security Operations Centers (SOCs) which offer cost-effective services for K-12 schools and train new cybersecurity professionals.

(6) Help schools hire expert staffing.

The CHAIR. Thank you very much.

Ms. Norris.

STATEMENT OF HELEN NORRIS, VICE PRESIDENT AND CHIEF INFORMATION OFFICER, CHAPMAN UNIVERSITY, ORANGE, CA

Ms. NORRIS. Let me begin by thanking, Chair Murray, Senator Cassidy, and the Members of the Committee for the opportunity to address you on this important topic. I am Helen Norris, the Chief Information Officer at Chapman University.

As the CIO, I oversee all technology for the institution, including our cybersecurity practice. Chapman is a mid-sized private university in Southern California with about 10,000 students. However, I have worked across a variety of institutions since 1997, including the University of California at Berkeley and the California State University.

Through my experience at these three universities, I have observed the cybersecurity threat landscape change over the years. When I arrived at Berkeley in 1997, we did not even have one IT professional that worked in information security.

Now, many colleges and universities have cyber—have large departments, have entire departments to deal with the threats that we face. We must defend against a variety of threats, including ransomware, phishing, hacking, and social engineering. We manage sensitive student financial and employee data.

Universities that include medical centers and teaching hospitals have even greater challenges in managing personal health information for individuals. Our systems have grown into complex environments that include large data center and growing—large data centers and a growing set of third party partners.cj

The scope and intensity of our operations presents challenges to keeping them secure, and we know that bad actors are always looking to turn our difficulties into their opportunities. As I describe cybersecurity challenges, however, I do want to note that higher education is not monolithic. There are approximately 6,000 institutions across the country and there is incredible variety among them.

The challenges related to cyber security differ across types of institutions, but there are some common themes. First, addressing cybersecurity threats is expensive. Investment in this area varies depending on the type of institution.

A large research university or one with a medical center might employ a good sized cybersecurity department. But a smaller university or a community college with more financial limitations will be challenged to do so, even though they must protect sensitive student data in a similar way.

Second, the complexity of this work is enormous. New threats emerge with alarming speed, and we must pivot to address them as they arise. The challenge is not just for our information security professionals. Cybersecurity threats impact our entire community. In higher education, we often say that cybersecurity is everyone's job, as we all face threats of ransomware, phishing, and hacking.

Institutions are also challenged by the increasing number and complexity of cybersecurity regulations, which generate costs that draw resources away from managing risks. My peers and I would welcome the chance to work with agencies to standardize and streamline requirements so we can focus our limited resources on maximizing cybersecurity. While the challenges we face are real and complex, higher education is sophisticated in cybersecurity threat mitigation and protection.

As noted, most institutions have added resources in this area to directly address risks. Our teams protect our networks and our systems in a variety of ways. Some of these involve technical measures like firewalls, encryption, and network segmentation. But much of the work these groups do is outreach to our community. Many security incidents occur when an individual falls into a trap set by a hacker.

A large part of our work is an education—is educational, ensuring that our students and others have the tools that they need to protect themselves. Colleges and universities also address cybersecurity by combining our strength through collaboration to protect the entire ecosystem. We share information on new threats, best practices, and community sourced tools.

We also work closely with partners in Federal and state agencies, particularly the FBI and CISA. Institutions want to continue to buildupon our response to the threats that are out there, and we see partnering at the Federal level as critical to that. We encourage continued and growing collaboration between our community and Federal agencies.

We also welcome ongoing dialog with this Committee as it considers further the cybersecurity challenges and opportunities we face. We believe that engagement and partnership with colleges and universities will help ensure effective approaches to bolstering cybersecurity.

With that in mind, I encourage you to reach out to colleges and universities in your states so that you can hear directly from them about their experiences and what would most help them to succeed in this critical area.

In closing, I want to thank you again for giving me the opportunity to address you, and I look forward to your questions.

[The prepared statement of Ms. Norris follows:]

PREPARED STATEMENT OF HELEN NORRIS

SENATE HELP COMMITTEE

CYBERSECURITY IN THE HEALTH AND EDUCATION SECTORS

TESTIMONY OF HELEN NORRIS

Chair Murray, Ranking Member Burr, and Members of the Committee,

Thank you for holding today's hearing on cybersecurity in the education and health sectors and for providing me with the opportunity to testify about the cybersecurity landscape in the higher education sector. My name is Helen Norris and I am the Chief Information Officer at Chapman University. As the CIO, I am responsible for all technology at the institution and oversee our cybersecurity practice. Chapman is a midsize private university, with about 10,000 students, in Southern California. However, I have worked in higher education across a variety of institutions since 1997, including UC Berkeley, a large research university, and the California State University.

I will focus my testimony today on cybersecurity threats and challenges in the higher education sector, the impact those threats have on a campus community, and the steps that cybersecurity professionals and their colleagues are taking to prevent, mitigate, and respond to these challenges.

Cybersecurity Threats and Challenges in Higher Education

The cybersecurity threat landscape has grown and transformed over the years. Colleges and universities are a target for hackers and need to defend against threats in the form of ransomware, hacking, phishing and social engineering as they manage sensitive data, including student data. We manage personal data pertaining to our employees, and financial data including

payment and banking information. Universities that include medical centers and teaching hospitals face an additional layer of cybersecurity considerations as they also manage personal health information.

It is important to understand that university data systems are highly complex environments to manage and that those systems have both grown in number and data content over recent years. This complexity accelerated even further during the pandemic, as we found ourselves supporting at-home work and a vastly increased online presence in teaching and research. These developments necessitated that we expand our "protection zone" beyond the institution's network to encompass a national or global workforce and student body. This is all within a diverse technical infrastructure that includes our data centers and third-party partners. Colleges and universities must keep these realities in mind as they evaluate and assess the cybersecurity threats that exist today and the challenges those threats pose to the campus community. The scope and intensity of our data operations presents challenges to keeping them secure, and we know that bad actors are looking every day for ways to turn our difficulties into their opportunities.

I would note that higher education is not monolithic. There are approximately 6,000 Title IV institutions across the country, and there is incredible variety amongst them, including community colleges, research institutions, HBCUs, small private institutions and so on. The challenges related to cybersecurity are different across these institutions, although there are some common themes.

First, the need to address cybersecurity threats is an expensive endeavor, particularly in a sector that faces other budget pressures, such as an across-the-board rise in costs, delays in the post-pandemic recovery of enrollments, and the need to maximize college affordability. It has

become necessary for universities to invest in this area, especially in terms of hiring information security professionals, as well as acquiring security tools and services. This investment varies depending on the type of institution. A large research university or one with a medical center might employ a good-sized information security department. But a smaller university or a community college with more financial limitations simply can't afford to do this, even though they must protect similar information on behalf of their students and their community. In addition to the cost of this operation, cybersecurity is a highly competitive field, and the nation as a whole simply does not have enough human resources currently to meet the demand. Universities are at a disadvantage in competing with employers in the tech sector when hiring information security professionals, where the jobs are better-paying and seem more attractive. It is difficult for higher education institutions to develop and retain a skilled cybersecurity workforce. One approach we have taken to addressing this challenge is to integrate our students into our workforce, an action that brings benefits for all.

In addition to the human resources needed to manage the risk, the complexity of the work is enormous. We are constantly dealing with new threats but also new and sometimes conflicting regulations and requirements. We have ever-growing lakes of data with privacy implications that must be protected. New threats are introduced with alarming speed, and we must pivot to address them as they arise. To manage these ever-growing threats, a variety of tools are developing in the marketplace. Universities need highly skilled-integration engineers and security experts to blend these tools together and implement the full monitoring, notification, and automated steps taken at each layer of our environment. Over time, we do expect artificial intelligence to improve the ability of these tools to deliver these protective actions more efficiently and independently.

Even more expensive than managing the risk is the cost of addressing an incident when one occurs. Ransomware is now among the most well-known types of security incident. In this situation, a hacker essentially "kidnaps" the victim's data by encrypting it and will only share the key to decrypt the data when a ransom is paid. While we don't have exact figures on how often this occurs in any sector, we know that a number of successful ransomware attacks, some very high profile, have occurred at colleges and universities. Ransomware attacks are usually carried out by offshore hackers, which makes addressing them even more challenging. It can be highly lucrative for these individuals, and usually there is very little risk to them with this activity. Ransomware tactics and techniques have continued to evolve in recent years, demonstrating threat actors' growing technological sophistication and an increased ransomware threat to organizations globally. For example, ransomware threat actors are now using double and triple extortion by threatening to:

1. Publicly release stolen sensitive information,
2. Disrupt the victim's internet access, and/or
3. Inform the victim's partners, shareholders, or suppliers about the incident.

Ransomware attacks on universities have been highly disruptive, shutting down the daily operations of the university until the ransom is paid, or the data can be recovered in other ways, a process that usually takes days or weeks. All of this is costly for colleges and universities in financial terms and is also highly disruptive for the institutional community that lacks access to those systems or data during this downtime. An article from the EDUCAUSE review included here as Appendix 1 illustrates some of the impact of a ransomware incident. Quoting from the article: "The impact of a ransomware attack can be devastating. For example, a West Coast university was the victim of a ransomware attack involving data within their school of medicine's

research department. After the university realized hackers had encrypted valuable research data, the school chose to pay the hackers $1.14 million in cryptocurrency in hopes that the hackers would provide a decryption key. Fortunately, the school reported that it received a key to restore access to the files and copies of the stolen documents. The FBI recommends against ever paying a ransom to ransomware attackers, as there is no guarantee that the data will be recovered, and paying the ransom encourages the hackers to repeat the attack. The FBI encourages victims of ransomware attacks to contact their local FBI field office to request assistance.

Most types of cyberattacks are happening globally. In England, a top university recently suffered a ransomware attack that forced the school to shut down nearly all of its IT systems. The school was forced to delay the start of the next term while IT teams scrambled to investigate the attack and determine the effect on their systems. The impact of ransomware is not always just a monetary loss, as the disruption to a school's term start will affect many other programs and schedules down the road."

Even when the security teams are successful in avoiding an interruption in services or paying a ransom, hacking incidents are still disruptive and time-consuming. In 2020 a university in California discovered that hackers had infiltrated its systems. While the team successfully shut down the initial attack immediately, they later learned that the cybercriminals had stolen passwords that gave them access to the campus systems for a much longer period.

As in other sectors, higher education is at risk of data breaches, often, as described above, as part of a ransomware attack. In most states, there is a requirement to notify individuals when certain aspects of their personal data have been exposed. This is indeed appropriate. However, it can be an expensive and disruptive process for the institution. In 2017, IBM and the Ponemon Institute

published research that showed that the average cost of a breach that involves data exposure can result in costs to the university of $245 per record. The financial impact of a significant breach, which may involve hundreds or thousands of records, can be devastating to a university.

Higher education institutions also face a complex regulatory environment in relation to cybersecurity. Recent revisions by the Federal Trade Commission (FTC) to its Safeguards Rule established under the Gramm-Leach-Bliley Act (GLBA) have greatly expanded the number and scope of requirements with which college and university cybersecurity programs must comply starting late this year. These new mandates are all the more pressing since Safeguards Rule compliance is also a condition of the agreement that institutions must sign to participate in Title IV Federal Student Aid programs authorized under the Higher Education Act. The revised Safeguards Rule directives delve deeper than ever before into institutional cybersecurity, applying to systems that are *connected* to systems that contain covered information and specifying particular human resources practices that institutions must adopt in relation to their information security staff, among many other things. While colleges and universities are working hard to meet the FTC's December deadline for compliance, many will certainly be challenged to address the significant expansion of Safeguards Rule requirements by the end of the year.

When releasing the new version of its regulations, the FTC also asked for public comment on a proposal to add an incident reporting requirement to the Safeguards Rule. The FTC has not yet indicated whether a final rule on this issue will be released or what its final form will be if so, but the higher education community was generally satisfied with the proposed regulation as initially presented. However, an additional incident reporting requirement from the FTC would exist alongside state data breach reporting requirements that vary across the 50 states. Higher

education institutions try to account for the current diverse array of reporting laws and regulations by designing institutional incident response and breach notification processes around their common elements. Differences still exist, though, and simply being prepared to track and address those differences in relation to any given incident carries with it significant administrative overhead. Therefore, additional reporting requirements, such as the FTC's proposed incident reporting requirement, that may themselves seem manageable in isolation should be understood as introducing more layers to an already tall stack of compliance measures that institutions have to follow, and those efforts present additional costs with which institutions, as well as students and other stakeholders, have to contend.

Colleges and universities also know that, in addition to complying with the Safeguards Rule, they will eventually be required by the U.S. Department of Education to follow the cybersecurity guidelines for "controlled unclassified information (CUI)" developed by the National Institute of Standards and Technology (NIST). This stems from the fact that "education records" as defined by the Family Educational Rights and Privacy Act (FERPA) are considered CUI under the National Archives and Records Administration (NARA) CUI Program established as a result of Executive Order 13556, "Controlled Unclassified Information." The Office of Federal Student Aid has previously stated that it considers Federal Student Aid data shared with institutions to facilitate the awarding and distribution of federal student financial aid to fall under the "education records" CUI category, and thus it intends to work toward ensuring institutional compliance with the NIST CUI guidelines in the years ahead. Institutions that conduct relevant research for the U.S. Department of Defense (DoD) must already follow these guidelines in relation to the DoD CUI (or covered defense information (CDI)) related to those projects, with

the guidelines also forming an integral part of DoD's Cybersecurity Maturity Model Certification (CMMC) Program. The application of the guidelines to student financial aid information, however, will greatly expand their scope of impact across colleges and universities as well as within institutions, given that the CUI requirements are associated with student financial aid data that will generally find its way into multiple institutional administrative systems. While many institutions have a working knowledge of the NIST CUI guidelines and may in fact be complying with them now, many others know that meeting the standards will be one more resource-intensive exercise on top of compliance efforts, such as fulfilling the new Safeguards Rule provisions, that are already underway. (Please see Appendix 2 for the supporting documents regarding the regulatory issues discussed in this and the immediately preceding paragraphs.)

Colleges and universities take compliance with federal and state cybersecurity requirements very seriously. Beyond regulatory compliance, we take even more seriously our obligation to our students, their families, and our stakeholder communities to secure the data with which we are entrusted and to provide secure environments in which learning, research, and service can take place. The ever-growing number and complexity of the compliance requirements that we face, however, presents an ever-expanding set of administrative burdens and associated costs that may detract from our capacity to manage the actual cybersecurity risks confronting our institutions, both now and in the future. Higher education technology and cybersecurity leaders would welcome the opportunity to explore with policymakers and regulators how these requirements might be streamlined to ensure that we can maximize the value of our cybersecurity resources to maximizing our cybersecurity effectiveness.

Impacts on students, staff, patients and families

Students are also directly and personally impacted by the disruption of an actual breach. Ransomware attacks can cripple the university's ability to operate by taking down critical systems for an extended period of time, as noted in the earlier example from the United Kingdom. During that time, students lose access to critical services that they need from the institution. This may include the ability to communicate with their faculty as well as the ability to manage their assignments and tests, directly impacting their educational experience. In some instances, colleges and universities have chosen to shut down all services, including canceling classes, until they are confident that they have eliminated the threat from the system or systems in question. Students are also impacted during a data breach if their own data is exposed, creating the risk of negative personal and financial impacts.

Incidents that impact individuals, however, are most often at a smaller scale than a major data breach or ransomware incident. Students in particular must be ever-vigilant to the ongoing attempts by hackers to trap them via email scams based on social engineering. There are many incidents in which a student "falls for" an email scam fraudulently offering a part-time job or threatening to share embarrassing personal information, and the student actually loses money in the process. These phishing attacks involve a hacker impersonating a trusted authority and convincing the victim to share his or her personal information, or even send money to the individual. Students are often victims of a particularly common form of this scam comprised of a fake job offer. In the past we have seen increases in this activity at specific times of the year, such as holidays or tax time, and higher education institutions are often and explicitly targeted.

How colleges and universities prevent, mitigate and respond to these challenges

While the challenges we face are real and complex, the higher education sector is sophisticated in cybersecurity threat mitigation and protection. As noted, most of us have invested resources to build effective cybersecurity capacity. Our information security teams deploy a variety of technologies and processes to protect institutional networks and systems. During the pandemic, as our staff, faculty and students all needed to work, teach, and learn remotely, colleges and universities had the need to implement and extend our technical protections to off-site locations. Some of the technical tools we use to respond to cybersecurity challenges are outlined below:

- Implementing multi-factor authentication to govern system access;
- End Point Detection and Response Systems (EDR), which protects systems both on and off the campus network;
- The use of technology such as firewalls to protect the physical network;
- Encrypting our most sensitive data;
- Network segmentation, which puts our more valuable and sensitive data in a more secure section of the network;
- Addressing software vulnerabilities by applying patches provided by our partners;
- Utilizing virtual private network (VPN) technology to encrypt data when it is accessed from a remote location;
- Using modern monitoring technology to root out suspicious activity on our networks and investigate those activities.

While we often tend to think of cybersecurity as focusing on technical solutions, it is in fact a very human issue and many of the efforts in colleges and universities to combat cybersecurity threats involve outreach to our stakeholders. For example, as previously noted, many security

incidents result from an individual falling into a trap set by a hacker through phishing. Higher education information security professionals strive to ensure that the members of our institutional communities have the tools to protect themselves from such incidents—tools that will help them recognize these traps and avoid them altogether, creating a strong **human** firewall for our institutions. Examples include:

- As noted above, implementing multifactor authentication to govern systems access and educating our community on its importance;
- Phishing campaigns designed to educate our students, faculty and staff on this risk; and
- General outreach and education, which includes sharing information about current threats.

Colleges and universities also address cybersecurity challenges by amplifying our strength through collaboration. As noted previously, there is a great variety in the type of institutions and how they are resourced. Less well-resourced colleges and universities may not individually have the level of human resources needed to manage the range of threats they face on their own. But the overall community comes together to protect the entire ecosystem. Through organizations like EDUCAUSE, Internet2 and REN-ISAC, we share information on new threats, best practices and community-sourced tools. In addition, we work closely with partners in many federal and state agencies, particularly the FBI and CISA. Many institutions develop relationships with their local FBI cybersecurity teams in advance of an incident. This collaboration helps us to avoid problems, and it also enables us to respond more quickly when an incident does occur. CISA offers a variety of free cybersecurity services and tools to colleges and universities, including an online database of known exploited vulnerabilities that is a critical tool, and even free vulnerability scanning. (https://www.cisa.gov/free-cybersecurity-services-and-tools) That means

that CISA will test an institution's internet-facing systems to find weaknesses. Literally hundreds of colleges and universities take advantage of these great services, and they are a critical part of our defense.

Finally, while we plan and protect, universities also prepare for the worst using several different techniques. Most universities have created incident response plans (IRPs) that outline what we should do in the event of a cybersecurity incident such as a ransomware attack. Universities generally test these plans on a regular basis via tabletop exercises that allow them to evaluate their preparedness for an event and adjust their plans as necessary. Some institutions also carry cyber insurance that aids them in the event of an incident, with their insurance carriers also providing guidance in the preparation and testing of an IRP. Unfortunately, cyber insurance has become prohibitively expensive for some institutions, and looking to the future, the growing cost of cyber insurance remains a concern for higher education as a whole.

In summary, colleges and universities usually take a multi-layered approach to security by:

- Utilizing technical tools to protect our networks and technical environments from unauthorized access by hackers;
- Using outreach, communication and education to protect our institutional communities from phishing for data and credentials, email scams and ransomware;
- Actively engaging with federal agencies and the higher education community in general to increase our own awareness of current threats and risks, allowing us to avoid becoming a victim of those new threats; and
- Preparing and planning for an incident should one occur.

In conclusion, I would again like to thank the Committee for your attention to this important issue. I look forward to continued collaboration and conversation on this topic.

APPENDIX 1

Why IT Matters to Higher Education
EDUCAUSE REVIEW

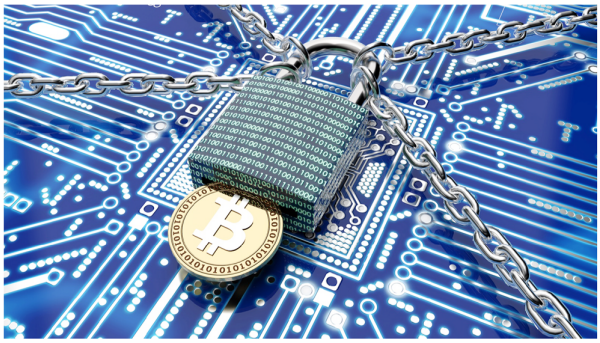
The Increasing Threat of Ransomware in Higher Education

Steve Scholz, **William Hagen** and Corey Lee Tuesday, June 22, 2021

Cybersecurity and Privacy

7 min read

Cyberattacks are increasing in frequency and impact. Defending against ransomware attacks requires a tiered approach to security with a Zero Trust model at the heart of the methodology.



Credit: posteriori / Shutterstock.com © 2021

During the pandemic, several major cyberattacks have unfolded, resulting in severe impacts to organizations and individuals. One of the most talked-about cyberattacks in 2020 was the SolarWinds breach, in which hackers gained access to nearly 18,000 clients of SolarWinds. The victims of the attack include Fortune 500 companies and multiple US government agencies.

In May 2021, Colonial Pipeline Company, a major refined-oil products supplier responsible for 45 percent of the East Coast's fuel supply, was hit in the largest-known hack to date on US energy infrastructure. The attack caused Colonial Pipeline to shut down its entire system, leading to panic and a disruption in gasoline supply across the East Coast of the United States.[1] In order to unlock encrypted files and get the pipeline back up and running, Colonial Pipeline paid hackers $4.4 million in Bitcoin for a decryption key.

Recently, the number of ransomware attacks similar to the attack on Colonial Pipeline has increased dramatically. The number of ransomware attacks more than doubled as cybercrime operations increased throughout the coronavirus pandemic. These attacks grew not only in frequency but also in sophistication and ransom demand. In 2018, the average ransom demanded from a victim was $8,000. In 2020, the average demand grew to $170,000, with high-end demands exceeding $1 million.[2]

Ransomware attacks are not only affecting businesses; colleges and universities are also prime targets for attacks. Surprisingly, education is the most affected sector for malware attacks when compared to other industries like business and professional services, retail and consumer goods, and high tech. Within the last thirty days, educational organizations have been the target of more than 6.1 million malware attacks, while the second-most affected industry (business and professional services) has only seen 900,000 attacks.[3] An analysis of ransomware campaigns within higher education found that ransomware attacks against colleges and universities have more than doubled since the onset of the coronavirus pandemic.[4]

The FBI's Cyber Division recently warned that ransomware poses a huge risk for higher education, as cybercriminals using this type of attack are now focusing heavily on colleges and universities.[5] The FBI became aware of a new type of ransomware attack—using a new type of malware known as PYSA—where unidentified cyber actors are specifically targeting higher education, K–12 schools, and seminaries. These actors use PYSA to exfiltrate data from victims prior to

encrypting the victims' systems to use as leverage in eliciting ransom payments.

What Is Ransomware?

Ransomware is a malicious form of malware, where hackers deploy a malicious computer code to block an organization's access to its own computer network to extort a ransom. The types and complexity of ransomware attacks have increased rapidly over time, and today many ransomware attacks see cybercriminals gaining access to an organization's data and then holding it hostage with military-grade encryption.

There are three main types of ransomware (listed below in order of increasing severity and complexity):

- **Scareware:** This type of ransomware typically includes rogue security software and tech-support scams. In this type of ransomware, the victim may receive a pop-up message claiming that malware was discovered on their system, and the only way to eradicate the malware is to pay for the security software to remove it. In most cases, this type of attack poses little actual risk to files and data.
- **Screen lockers:** When a screen locker attack is deployed, the victim is locked out of their computer entirely. Upon startup, a full-size window will appear demanding ransom payment and prohibiting the victim from using their computer.
- **Encrypting ransomware:** This is the most complex and devastating type of ransomware. Cybercriminals will gain access to the victim's system, seize their files,

encrypt them, and then demand payment for decrypting and returning the files.

When faced with an encryption ransomware attack, the victim is left with only a few choices: they can either pay a ransom to the criminals (which does not guarantee the criminals will return the data), attempt to break the encryption on their data, or restore their data and systems from backups.

In a ransomware attack, hackers typically search out an organization's most valuable data. High-profile ransomware attacks sometimes target organizations that are conducting research where the data is highly confidential. In other cases, the data the attackers might be after could be confidential data about a university's students, including social security numbers, addresses, and birthdates. Another common target for ransomware attacks is any type of data or system that could make it impossible for an organization to function. Because of the data they possess, higher education institutions are key targets for ransomware attacks.

However, even smaller universities and colleges, as well as those without an emphasis on research, are prime targets for this type of cyberattack. Regardless of whether an institution considers its data to be valuable, chances are that cybercriminals do. Higher education institutions inherently gather and store large amounts of confidential student data and therefore must protect themselves against ransomware attacks.

Even more concerning than traditional malware-based ransomware attacks are human-operated ransomware attacks,

which pose a huge threat to organizations of all types. An advanced type of ransomware, human-operated ransomware attacks are becoming more frequent and costly. In a human-operated attack, a cybercriminal is actually controlling the attack in real-time, and after gaining access to a victim's system, the criminal quickly scans through files and locations—while also preventing any antivirus alerts—to pinpoint and steal the most valuable data.

In these types of attacks, the attacker will often exhibit extensive knowledge of systems administration and common network security misconfigurations, perform thorough reconnaissance, and adapt to what they discover in a compromised network. Existing antivirus solutions are often not a strong enough defense when an organization is faced with this type of hands-on-keyboard ransomware attack.

The Impact of Ransomware Attacks

The impact of a ransomware attack can be devastating. For example, a West Coast university was the victim of a ransomware attack involving data within their school of medicine's research department. After the university realized hackers had encrypted valuable research data, the school chose to pay the hackers $1.14 million in cryptocurrency in hopes that the hackers would provide a decryption key. Fortunately, the school reported that it received a key to restore access to the files and copies of the stolen documents. The FBI recommends against ever paying a ransom to ransomware attackers, as there is no guarantee that the data

will be recovered, and paying the ransom encourages the hackers to repeat the attack. The FBI encourages victims of ransomware attacks to contact their local FBI field office to request assistance.

Most types of cyberattacks are happening globally. In England, a top university recently suffered a ransomware attack that forced the school to shut down nearly all of its IT systems. The school was forced to delay the start of the next term while IT teams scrambled to investigate the attack and determine the effect on their systems. The impact of ransomware is not always just a monetary loss, as the disruption to a school's term start will affect many other programs and schedules down the road.

Developing a Strategy to Help Prepare for Ransomware Attacks

Defending against ransomware attacks requires a tiered approach to security with a **Zero Trust model** at the heart of the methodology. So, how does Zero Trust work? Zero Trust follows three guiding principles: verify explicitly, use least privileged access (LPA), and assume breach.

- **Verify explicitly:** Zero Trust closes gaps in multi-factor authentication (MFA) coverage by requiring explicit verification across the network. Instead of assuming trust based on weak assurances like network locations, Zero Trust uses all available data—identity, endpoint, and network data—to authenticate all access requests,

no matter where they came from or what they're accessing.

- **Use least privileged access (LPA):** Zero Trust makes it harder for attackers to negatively impact key systems and data by limiting users' access to the resources, devices, and environments they need. Without widespread privileges and access, attackers have fewer opportunities to move laterally within the network beyond an initial breach.
- **Assume breach:** As a final fail-safe, Zero Trust operates under the assumption that a breach has already happened or soon will. This means deploying redundant security mechanisms, collecting system telemetry, using that telemetry to detect anomalies, and—wherever possible—automating insight generation to enable near-real-time prevention, response, and remediation.

IT professionals play an important role in security and are the foundation of an approach to preventing ransomware. Many observed ransomware attacks leverage malware and tools that are easily detected by antivirus security software. Observed affected servers also often lack firewall protection and MFA, have weak domain credentials, and use non-randomized local admin passwords.

Oftentimes, these protections are not deployed because there is a fear that security controls will disrupt operations or impact performance. IT professionals can help determine the true impact of these settings and collaborate with security teams on mitigations. Attackers often prey on settings and configurations that many IT admins manage and control. Given

the key role they play, IT professionals should be part of security teams to defend against ransomware attacks.

When considering complex, human-operated ransomware attacks, traditional solutions like MFA and antivirus are a good start but will not completely defend an organization against a knowledgeable cyberattacker. The only way to defend against these types of events is a twofold approach involving top-of-the-line endpoint detection and response paired with a user entity behavior analytics (EUBA) solution. This is the only way to pinpoint if there is an attacker on the inside of a system who has managed to evade or silence antivirus alerts.

Microsoft has the tools and expertise needed to ensure your security system is able to prevent ransomware attacks.

Contact your Microsoft account representative to discuss your security needs and learn how higher education institutions are defending against ransomware attacks.

Additionally, you can learn more about Microsoft's approach to defending against these types of cyber-attacks and **human-operated ransomware on Microsoft Docs.**

Notes

1. Will Englund and Ellen Nakashima, **"Panic Buying Strikes Southeastern United States as Shuttered Pipeline Resumes Operations,"** *Washington Post,* May 12, 2021. ↩

2. John Leyden, **"Ransomware Attacks More Than Doubled Last Year as Cybercrime Operations Scale Up during Coronavirus Pandemic,"** The Daily Swig (website), March 8, 2021. ↩
3. Microsoft Security Intelligence, **Global Threat Activity Map by Industry,** Microsoft (website), accessed June 4, 2021. ↩
4. ***Cybersecurity in Higher Education,*** research report, (New York, NY: BlueVoyant, February 2021). ↩
5. Federal Bureau of Investigation Cyber Division, **Increase in PYSA Ransomware Targeting Education Institutions,** FBI FLASH, Alert Number CP-000142-MW, March 16, 2021. ↩

Steve Scholz is Principal Technical Specialist for Security, Compliance and Identity, US Education, at Microsoft.

Bill Hagen is a Senior Director of Security addressing industry, partner, and customer requirements at Microsoft.

Corey Lee is Senior Consultant and Zero Trust Architect at Microsoft.

Microsoft is a supporting partner of EDUCAUSE.

Cyber Threat Intelligence, Cybersecurity, Encryption, Endpoint Detection and Response (EDR), Incident Management and Response, Intrusion Detection and Prevention, Security Risk Management, Vulnerability Management, Zero Trust

APPENDIX 2

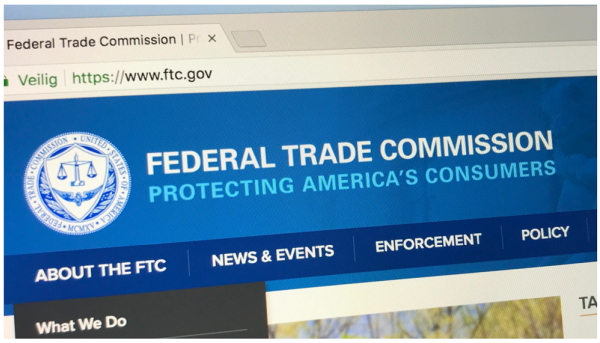
Why IT Matters to Higher Education
EDUCAUSE REVIEW

Policy Analysis: Revised, Highly Prescriptive FTC Safeguards Rule

Jarret Cummings Thursday, December 2, 2021 Policy

20 min read

The Federal Trade Commission (FTC) has released a revised version of the Safeguards Rule. The revised Rule will impose many new requirements on institutional cybersecurity operations in relation to student financial aid and other "customer" information.



Credit: Jarretera / Shutterstock.com © 2021

Note: The Federal Trade Commission officially published its revised Safeguards Rule in the *Federal Register* on December 9, 2021, making December 9, 2022, the deadline for institutions to achieve compliance with the new requirements of the revised Rule. **The text below has been updated as of March 9, 2022, to reflect this change.** Some of the document links have been revised as well to reflect new, post-publication locations of the respective resources.

When the Federal Trade Commission (FTC) proposed to **revise** the Safeguards Rule (the Rule) in 2019, EDUCAUSE joined with the American Council on Education (ACE) and several other associations to submit **comments** asking for a number of changes and clarifications.[1] Those comments derive largely from an **analysis** (written by EDUCAUSE members and staff) of the FTC's proposed revisions to the Rule.[2] In light of the

initial comments that the FTC received, including ours, the agency held an online listening session during the summer of 2020. Among the select stakeholder panelists the FTC invited to participate were a few EDUCAUSE member CIOs and CISOs. However, the FTC did not provide any insights into how the feedback it received on its proposed rulemaking might influence the form that its revised cybersecurity regulations would take. The agency **released** the latest version of the Safeguards Rule on October 27.[3] This version is largely unchanged from the FTC's original draft. *(Note: The pre-publication draft originally made available by the FTC on October 27, 2021, was replaced by a pre-publication version posted to the online version of the Federal Register on December 8, 2021. The references and links to the pre-publication draft of the revised Rule have been updated to reflect the December 8 version in the online Federal Register since that is the pre-publication form of the document still available. The same is true for the supplemental notice of proposed rulemaking regarding a possible Safeguards Rule reporting requirement. The December 8 version of that document is the pre-publication version still available, so relevant references and footnotes have been updated accordingly.)*

Given the extensive edits, clarifications, and changes that we requested,[4] the FTC's decision not to substantially revisit its regulatory proposal is disappointing. That said, the analysis of public comments provided with the FTC's **pre-publication copy** of the new Rule contains an important acknowledgment from the agency that sets the context for interpreting and applying the numerous provisions with which colleges and universities will now have to comply:

> Although the Final Rule has more specific requirements than the current Rule, it still provides financial institutions the flexibility to design an information security program that is appropriate to the size and complexity of the financial institution, the nature and scope of its activities, and the sensitivity of any customer information at issue.[5]

This statement is significant because it is relevant to a point that EDUCAUSE and our higher education association partners pressed throughout our comments on the proposed Rule. We consistently noted that many provisions lacked sufficiently specific guidance to assure a college or university that it had achieved compliance, an issue that we summarized as follows:

> The proposed revised Rule, however, specifies many of the details of those elements while adding more provisions and requirements, but without providing effective guideposts for compliance. That leaves colleges and universities with many questions about whether the proposed Rule's provisions are appropriately limited to the data and functions it covers and how institutions will effectively be able to determine if they are in compliance regardless.[6]

The statement from the FTC quoted above directly addresses this concern.[7] In my view, it reaffirms that an effective approach to the requirements of the Safeguards Rule, including all of its new provisions, remains a matter of discretion for the covered entity in question based on its size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles. The Rule identifies the elements that an institution's information security

program must include; however, it leaves the determination of how the institution should address those elements (for the most part) to the covered entity, with the understanding that the institution will make those decisions based on, and reasonably justified by, its particular context.

From a compliance standpoint, institutions may view this level of discretion as a double-edged sword based on understandable concerns about their decisions being second-guessed by regulators at some point in the future. Given the FTC's position as reflected in the acknowledgment from the agency quoted above and its analysis of public comments on the proposed revisions to the Rule, institutions may best respond by adopting an approach that EDUCAUSE asked the FTC to affirm explicitly in the Rule or its related guidance (which it apparently declined to do in favor of reaffirming the extent of institutional discretion):

> [W]e would urge the FTC to explicitly state in the Rule and subsequent guidance what we believe the proposed revised Rule implies—that institutions may achieve compliance through providing reasonable explanations in their information security program documentation for the choices they make in fulfilling the given provisions.[8]

In other words, the discretion to determine what constitutes an appropriate way to fulfill a given requirement based on an institution's size and complexity, the nature and scope of its activities, and so forth carries with it the responsibility of ensuring that the measures adopted by the institution are appropriate given what it is, what it does, and what options it may reasonably have available to it as a result.

I used the word "regulators" above, not "the FTC," because the Office of Federal Student Aid (FSA) at the US Department of Education (ED) has made compliance with the FTC Safeguards Rule a requirement of the Title IV Program Participation Agreement (PPA) that institutions must sign to participate in federal student financial aid programs.[9] As a result, institutions are ultimately responsible to the FTC directly for complying with the Safeguards Rule, but a determination by FSA that an institution is not complying with the Safeguards Rule may affect its Title IV eligibility and therefore the ability of the students enrolled at the institution to get federal student loans and other forms of federal financial aid.

It remains unclear how FSA will address the changes in the FTC's cybersecurity regulations. Conversations between EDUCAUSE and FSA representatives about the issues that have occurred since the FTC unveiled its rulemaking notice in 2019 did not produce any indication of how FSA would incorporate Safeguards Rule revisions into its compliance expectations. For now, the **Safeguards Rule audit objective** that FSA had incorporated into the federal single audit process still focuses on confirming a few high-level objectives from the previous version of the Rule:

- That an institution has appointed a person or team to coordinate its information security program
- That it has conducted a relevant risk assessment
- That it has developed information security controls based on its identified risks[10]

FSA will have to work with the Office of Management and Budget to alter the audit objective in light of the FTC's revisions to the Rule, if and when it chooses to do so, and that process will take time.

Meanwhile, EDUCAUSE intends to work with its members and association partners to engage with FSA to understand its Safeguards Rule compliance and audit objective plans as they take shape. We hope such discussions will also provide the opportunity for member representatives to share information about the practical issues and difficulties that different approaches to FSA compliance in this area might present. In this regard, FSA is better positioned to understand the problems that the revised Rule creates for colleges and universities and to tailor its compliance interests to the higher education context.

Turning to the revised Rule itself, even with the understanding that how an institution fulfills a given requirement remains discretionary, the long list of new requirements is still eye-opening. Also, the FTC is now requiring the adoption of several measures that EDUCAUSE argued in 2019 should continue to fall under institutional discretion. In the review that follows, I highlight what I consider to be key points in the revised Rule. I encourage EDUCAUSE members involved in their institution's compliance with the Safeguards Rule to review the **revised regulations** in their entirety (see pp. 109–128 for the text of the new Rule itself), as some parts of the Rule may be more central to your institution's needs and interests than the ones I identify below.

In addition to releasing the revised Safeguards Rule, the FTC also announced that it would conduct a **supplemental**

rulemaking on the issue of whether to require entities covered by the Rule to report relevant cyber incidents to the FTC.[11] The higher education comments on the proposed Rule that EDUCAUSE helped to develop in 2019 raised questions about the value of such a reporting requirement, especially as it relates to the burden that the requirement would create for covered entities such as colleges and universities. The new FTC rulemaking notice indicates the agency's desire to minimize the potential burden of Safeguards Rule incident reporting, which may, in turn, lessen higher education's concerns about a proposed requirement. I will be writing a supplemental article in which I review the need to consider whether EDUCAUSE and the higher education community should submit comments on the FTC's proposed incident reporting requirement and, if so, the direction those comments should take. *(Note: The review of the rulemaking notice regarding a possible Safeguards Rule reporting requirement was posted on **December 8, 2021**. EDUCAUSE joined several associations in submitting comments about the proposed reporting requirement to the FTC on February 7, 2022. An article reviewing the higher education submission, with a link to the comments themselves, was posted on **March 3, 2022**.)*

The Revised FTC Safeguards Rule: Key Provisions by Section

Please note that the *Code of Federal Regulations (CFR)* reference for the Safeguards Rule is **16 CFR 314.** To find the Safeguards Rule regulations, enter "16 CFR 314" in the search bar on the **Electronic Code of Federal Regulations** web page.

Section 314.5—Effective Date

Keep in mind that most of the new requirements added to the Rule will not take effect until one year after the date of their publication in the *Federal Register. (Note: The revised Safeguards Rule was officially published in the Federal Register on December 9, 2021, and it identifies December 9, 2022, as the compliance deadline for the new requirements incorporated into the revised Rule.)* With that in mind, I will take the second-to-last section, Section 314.5—Effective Date, out of order since it identifies the following sections as falling under the one-year compliance deadline:

- 314.4(a)—Designate a "qualified individual" to oversee, implement, and enforce the institution's information security program.
- 314.4(b)(1)—Produce a written risk assessment about the institution's customer information that includes a now-mandated set of criteria and requirements.
- 314.4(c)(1)-(8)—"Design and implement safeguards to control the risks you identity through risk assessment," including the following:
    - Technical and physical access controls to ensure only authorized access
    - An inventory of all relevant parts of the IT environment and management of the same consistent with their business priority and the institution's risk strategy
    - Encryption of all customer information in transit over external networks and at rest

    - Procedures for securely developing internal applications and assessing the security of externally developed applications used in relation to customer information
    - Multi-factor authentication for *any* individual accessing *any* information system
    - Procedures for the secure disposal of customer information that is no longer needed for business operations or another legitimate business purpose
    - Change management procedures
    - Measures to monitor and log the activities of authorized users and to detect their unauthorized access or use of or tampering with customer information

- 314.4(d)(2)—Implement continuous monitoring of "information systems" (as defined in 314.2) or annual penetration testing with vulnerability assessments at least every six months.
- 314.4(e)—Establish policies and procedures to ensure that your staff receives security awareness training, that you hire qualified information security personnel and provide ongoing professional development for them, and that key members of your information security staff maintain their knowledge of current threats and responses.
- 314.4(f)(3)—Periodically assess the information security risks that your institution's service providers present and the adequacy of the safeguards they

deploy to ensure that they are following the provisions of the Rule.

- 314.4(h)—Establish a written incident response plan, including a set of specific elements, for the customer information that the institution controls.
- 314.4(i)—Require your institution's "qualified individual" to submit a written report on key aspects of the information security program to the institution's governing board at least once per year.

All other aspects of the revised Rule take effect thirty days from its publication in the *Federal Register*, but those aspects essentially concern the current requirements of the Safeguards Rule with modest text edits to accommodate the range of new requirements that will go into effect next year. In other words, the thirty-day deadline for the rest of the revised Rule ensures that covered entities continue to comply with pre-existing requirements while preparing to comply with the new ones. *(Note: The revised Rule officially took effect on January 10, 2022; as mentioned, though, the FTC has deferred compliance with the new requirements added to the Safeguards Rule until December 9, 2022.)*

Section 314.2—Definitions

- The FTC greatly expands the definitions section—largely to incorporate key terms from its Privacy Rule directly into the revised Safeguards Rule. These terms are important for understanding what the Safeguards Rule covers.

- For example, where the current regulation includes only the definition of "customer information," the revised Rule includes definitions of terms ("consumer," "customer," "nonpublic personal information," "personally identifiable financial information," and so forth) that are central to understanding what "customer information" actually means.
- EDUCAUSE and its partners specifically requested that the FTC add all relevant definitions from the Privacy Rule to the new Safeguards Rule to make it easier for institutions to understand what "customer information" they need to protect under the Rule, so this change, even at the expense of the Rule's brevity, is greatly appreciated.
- That said, IT leaders and professionals will likely be well served by working with institutional legal counsel as well as their business offices, registrars, and financial aid colleagues to walk through the interlocking chain of definitions that have to be explored to reach a full understanding of exactly what institutional data constitutes "customer information."
- Since institutions currently must comply with the existing version of the Safeguards Rule, most, if not all, probably already have a good handle on the scope of "customer information." However, with all of the relevant definitions now being included in the Rule itself, evaluating

the new compliance requirements presents a good opportunity to review the previous determinations to ensure nothing has been missed.

- **"Authorized user"**
  In the revised Rule, the FTC added "customer" to the definition's list of people who might be considered "authorized users" to make clear that the Rule's requirements for multi-factor authentication and user activity monitoring and logging, for example, extend to "customers" that can access their information via the institution's systems.

  Depending on how an institution already allows students to access their financial aid and institutional account information, the Rule's new security requirements may or may not pose problems. However, institutions will have to review those requirements in light of students' (or parents') access to account information and make sure all of the required measures are in place in ways that are appropriate to the institution's size, complexity, and so forth.

- **"Encryption"**
  In commenting on the proposed Rule, EDUCAUSE and its partners suggested that the FTC add to the definition of "encryption" to link the potential new encryption requirement under the Rule to "industry standards," which would give institutions a frame of reference for complying with the requirement. Instead, the final version of the revised Rule includes a

reference to "current cryptographic standards" as an appropriate measure to secure an associated encryption key.

From a compliance standpoint, I think the end result is the same. In deciding what form of encryption to deploy to meet the Rule's requirement, institutions should document how the method(s)/tool(s) that are chosen reflect current encryption standards and approaches.

- **"Information system"**
  As previously mentioned, one of the key definitional changes from the proposed Rule to the Final Rule is the addition of references to "containing customer information or connected to a system containing customer information" in the definition of "information system." As a result, the definition now clearly links systems and related technology covered by the revised Rule's requirements to the customer information for which institutions are responsible under the Safeguards Rule. However, as also noted previously, the addition of "connected to a system containing customer information" likely pulls a much greater degree of an institution's IT environment into the scope of the Rule's requirements than a college or university would find helpful or, in many cases, justified.

  This definitional change may point the way, though, to how an institution can modify its IT environment to segregate its "customer information" (with student financial aid and account information likely drawing the lion's share of concern) to limit the extent of the

environment that will fall under the Rule's new requirements, such as continuous monitoring or annual penetration testing or biannual vulnerability assessments. There is little doubt, however, that the FTC did not take into account our points about the extent to which student financial aid information might reasonably be distributed across institutional systems and, therefore, the difficulty that the scope of compliance in the revised Rule might pose for a college or university.

Section 314.4—Elements [of a Safeguards Rule-Compliant Information Security Program]

- **"Qualified individual" to oversee/enforce the information security program [314.4(a)]**
  The revised Rule follows the proposed Rule in moving from requiring that an employee or employees be designated to coordinate the institution's information security program to mandating that a single "qualified individual" be appointed to oversee, implement, and *enforce* the program. In our comments on the proposed Rule, we argued that the decision of whether to have individual or team leadership of an institution's information security program should remain a matter of institutional discretion given the great variety of institutional contexts. The FTC determined, however, that streamlining and ensuring accountability by having a single head of the information security program trumped other considerations.

That said, we also noted in our comments on the proposed Rule that the FTC's repeated reference to a chief information security officer in this context, which the agency intended to be just an example, would likely be interpreted as a mandate that all institutions might not be able to address within the anticipated timeframe for achieving compliance. With our feedback and similar comments from other stakeholders in mind, the FTC adjusted its text in the final rule so that it only refers to the need for an institution to appoint a "qualified individual" to lead the information security program. What constitutes being "qualified" will remain subject to institutional discretion based on the institution's size and complexity, the nature and scope of its operations, and so forth.

- **Risk assessment [314.4(b)]**
    - Under the revised Safeguards Rule, institutions will now have to develop a written risk assessment regarding the security of their customer information. The written assessment will have to cover the following elements:
        - The criteria used to evaluate and classify the relevant security risks that the institution has identified
        - The criteria used to assess "the confidentiality, integrity, and availability of your information systems and customer information, including the adequacy of the existing controls in the

context of the identified risks or threats you face"

- The ways in which "identified risks will be mitigated or accepted based on the risk assessment and how the information security program will address the risks"

- The expanded risk assessment requirement in the revised Rule also mandates that institutions periodically update their risk assessments, with when and how to do so left to institutional discretion based on institutional size, complexity, nature, scope, etc.

- **Safeguards [314.4(c)]**
  - The revised Rule goes into much greater detail about the types of security measures that institutions will need to implement to address the risks they identify in their risk assessments. In fact, one could interpret the specific requirements introduced as the FTC setting minimum baselines under the assumption that any valid risk assessment would identify the risks requiring the measures that the FTC is now imposing by regulation.
  - Under the revised Rule, institutions must take the following actions:
    - Implement and maintain technical and physical access controls on customer information to limit access to authorized

users and limit those users' access to the scope of their authorizations.

- Inventory and manage "the data, personnel, devices, systems, and facilities" central to their operations in light of their priority and the institution's "risk strategy."
- Encrypt all customer information "held or transmitted" by the institution when "in transit over external networks or at rest."
    - The FTC had previously raised the possibility of requiring encryption of customer information while in transit over *internal* networks as well, so this encryption provision could have been even more cumbersome to manage.
    - The provision also allows for institutions to use "effective alternative compensating controls" when necessary if approved by their "qualified individual."
- Adopt secure development practices for any internally developed applications and security assessment procedures for any externally sourced applications that

the institution uses to "transmit, access, or store customer information."

- **"Implement multi-factor authentication for any individual accessing any information system** [emphasis added], unless your Qualified Individual has approved in writing the use of reasonably equivalent or more secure access controls."
- Establish policies and procedures for the secure disposal of customer information "no later than two years after the last date" on which the information was used to serve the customer in question unless it is needed for business operations or "for other legitimate business purposes."
    - The institution may also maintain the data if required by law or regulation, or if it is held in a fashion that makes "targeted disposal . . . not reasonably feasible."
    - In responding to the proposed Rule, EDUCAUSE and its partners argued that "business purposes" might not be understood as the FTC intended in institutions focused on academic purposes, and thus it

should use the phrase "legitimate purposes."

- Since the FTC did not take our suggestion, institutions will have to rely on their discretion based on their size, complexity, nature, scope, etc., to determine what constitutes a "legitimate business purpose" given their operations.
- Also, this provision assumes that secure disposal of customer information as required will be based on a periodically reviewed and updated institutional data retention policy designed "to minimize the unnecessary retention of data."

- Adopt change management procedures (presumably for systems, policies, processes, etc., that connect in some meaningful way with customer information).
- Implement measures to "monitor and log the activity of authorized users" and to detect when they have accessed, used, or tampered with customer information outside the scope of their authorization.

        - The logging aspect of this provision replaces a separate provision in the proposed Rule that would have required the creation of "audit trails . . . to detect and respond to security events."
        - EDUCAUSE member feedback indicated that simply focusing on user logs would be a more accurate and useful way to address the FTC's concern, and it seems that our comment about the issue in relation to the proposed Rule led to an appropriate change.

- **Monitoring and testing safeguards [314.4(d)(1) and (2)]**
    - Part 1 of this provision requires institutions to test regularly or otherwise monitor the effectiveness of the safeguards established under their information security program "including those to detect actual and attempted attacks on, or intrusions into, information systems" as defined by the Rule.
    - Part 2, however, specifically mandates either continuous monitoring of information systems (again, as defined by the Rule) or annual penetration testing with vulnerability assessments at least every six months and

whenever the institution experiences significant operational changes or an incident that "may have a material impact on [the institution's] information security program."

- In commenting on the proposed Rule, EDUCAUSE and its partners argued that if, when, where, and how these measures might be deployed should be a matter of institutional discretion based on the findings of the institution's risk assessment in light of its size, complexity, nature, scope, etc., especially given the diversity of institutional types and contexts across higher education.
- In light of how the Rule defines "information system," limiting the reach of this provision across the institutional IT environment will require careful consideration of where and how customer information is stored and used, as well as which systems and data stores have to be connected to systems and databases containing customer information.

- **Human resources policies and procedures related to information security [314.4(e)]**
  - This aspect of the revised Rule requires institutions to provide security awareness training for their personnel consistent with the results of their risk assessments.
  - Institutions must also do the following:
    - Use qualified information security personnel to manage security risks and

"perform or oversee" their information security program, whether such personnel are institutional employees or are supplied by a service provider.

- Ensure their information security personnel have access to security updates and training that will allow them to address security risks at their institution.
- Verify that "key information security personnel" are maintaining their professional knowledge of the field (i.e., of "changing information security threats and countermeasures").

- **Service provider oversight [314.4(f)]**
  The revised Rule adds a requirement that institutions periodically review the information security risks that their relevant service providers pose, including the adequacy of those providers' safeguards.

- **Evaluation and revision of the information security program [314.4(g)]**
  The FTC changed this section from the proposed rule to the final rule to cross-reference the requirement about reviewing and revising the institutional information security program with the sections on modifying relevant safeguards based on the results of the institution's written risk assessment [314.4(b)(2)] and its continuous monitoring/annual penetration testing (with at least biannual vulnerability assessments) of relevant information systems [314.4(d)].

- **Written incident response plan [314.4(h)]**
    - The FTC revised this provision slightly in the revised Rule from how it was presented in the proposed Rule.
        - Rather than saying that covered entities have to develop written incident response plans to cover customer information in their "possession," the text now reads that they must have incident response plans for such information under their "control."
        - This edit responds to our comment on the proposed Rule regarding the need to revise this provision to reflect institutional use of cloud services, where the relevant information may actually be possessed by a cloud services provider and not by the institution directly.
        - Whether "control" works better than "possession" in this context remains debatable. We suggested that the text tie the incident response plan to the customer information for which the institution is "responsible," since there is little doubt that the covered entity remains responsible for the security of its data no matter where it is housed, especially in light of the Rule's service provider oversight provision.
        - To that end, regardless of how the text reads, the FTC's intent is clear: The

institution's incident response plan regarding covered customer information must account for relevant service providers as well.

- The provision identifies several specific items that a compliant incident response plan must include, all of which are consistent with standard incident response principles and practices.
- Institutions with incident response plans that cover customer information should review the list to establish a crosswalk between their plans and the required elements. Those needing to develop such plans should review the list to ensure that their plans cover all the bases.

- **Board reporting [314.4(i)]**
  - The revised Rule incorporates the proposed Rule requirement that the head of the institution's information security program submit a written report about the program to the institution's governing board at least once a year.
  - The modest edits to the provision in the revised Rule identify the head of the information security program as its "qualified individual" and specify that written reports should be provided to the board "regularly and at least annually."

- A Rule-compliant board report must include the following elements:
  - A review of the program's overall status and compliance with the Rule
  - "Material matters" about the program, such as:
    - risk assessment and risk management/control decisions;
    - service provider arrangements;
    - results of testing and security events or violations, and management's responses to them; and
    - recommendations for program changes.

Section 314.6—Exceptions

- Institutions that maintain customer information on fewer than 5,000 consumers (note the difference between "consumer" and "customer" in the definitions) are exempt from having to:
  - develop a written risk assessment [314.4(b)(1)];
  - implement continuous monitoring or penetration testing/vulnerability assessments of their information systems [314.4(d)(2)];
  - develop a written incident response plan [314.4(h)]; or

    - submit a report about their information security program to their governing board or senior executive [314.4(i)].

- In commenting on the proposed Rule, EDUCAUSE and its partners argued that the threshold for exceptions to the requirements of the Rule for higher education institutions should be set by Carnegie classification, not the number of consumer records managed, as Carnegie classification would provide a more appropriate indicator of institutional size (and therefore institutional capacity to manage the requirements in question). With the FTC declining to accept that recommendation, even the smallest accredited colleges and universities are unlikely to qualify for the exceptions to certain Rule requirements given the length of time for which financial aid and student account information is generally maintained.

Notes

1. Federal Trade Commission, **"Standards for Safeguarding Customer Information (Notice of Proposed Rulemaking; Request for Public Comment),"** *Federal Register*, Vol. 84, No. 65, April 4, 2019, pp. 13158-13177; Jarret Cummings, **"Higher Ed Community Responds to Proposed Safeguards Rule Change,"** *EDUCAUSE Review*, August 14, 2019. ↩
2. Please see Jarret Cummings, **"Safeguards Rule Comments Deadline Extended to August 2,"** *EDUCAUSE Review*, June 7, 2019, for more details. ↩

3. Federal Trade Commission, **"FTC Strengthens Security Safeguards for Consumer Financial Information Following Widespread Data Breaches,"** October 27, 2021. ↩
4. For details, see Jarret Cummings, **"Safeguards Rule Comments Deadline Extended to August 2,"** *EDUCAUSE Review,* June 7, 2019, and Jarret Cummings, **"Higher Ed Community Responds to Proposed Safeguards Rule Change,"** *EDUCAUSE Review,* August 14, 2019. ↩
5. Federal Trade Commission, **"16 CFR Part 314: Standards for Safeguarding Customer Information (Final Rule),"** pre-publication copy, (December 8, 2021): 5. ↩
6. American Council on Education et al., letter to the Federal Trade Commission, **"Request for Public Comment on Notice of Proposed Rule-Making, 'Standards for Safeguarding Customer Information' (Safeguards Rule, 16 CFR 314, Project No. P145407),"** August 2, 2019, 3. ↩
7. FTC, **"16 CFR Part 314: Standards for Safeguarding Customer Information (Final Rule),"** 5. ↩
8. American Council on Education et al., letter to the FTC, **"Request for Public Comment on Notice of Proposed Rule-Making,** 3. ↩
9. **"Record Keeping, Privacy, and Electronic Processes,"** in ***2021-2022 Federal Student Aid Handbook in PDF Format,*** (Washington DC: Office of Federal Student Aid, US Department of Education, 2021), 2-218, 2-220. ↩

10. Jarret Cummings, **"The Safeguards Rule Audit Objective Is Here!"** *EDUCAUSE Review*, July 11, 2019. ↩
11. Federal Trade Commission, **"16 CFR Part 314: Standards for Safeguarding Customer Information (Supplemental Notice of Proposed Rulemaking),"** pre-publication copy, (December 8, 2021). ↩

Jarret Cummings is Senior Policy Advisor at EDUCAUSE.

Compliance, **Cybersecurity Policy**, **Data Security**, **Encryption**, **Federal Student Aid**, **Higher Education Policy**, **Policy and Law**

Why IT Matters to Higher Education
EDUCAUSE REVIEW

Higher Ed Responds to Proposed Safeguards Rule Reporting Requirement

Jarret Cummings Thursday, March 3, 2022 Policy

5 min read

The Federal Trade Commission (FTC) has proposed adding a reporting requirement to its Safeguards Rule. EDUCAUSE and its partners recommend that the FTC adopt a few revisions (e.g., delaying the public release of any Safeguards Rule security event report for one year from the submission date).

The Federal Trade Commission (FTC) published its long-awaited revisions to the Safeguards Rule in early December 2021 while giving covered entities, such as colleges and

universities, until December 2022 to achieve compliance with the many new provisions of the Rule.[1] At the same time, the FTC also proposed a new Safeguards Rule reporting requirement. Comments on the proposal were due by February 7.[2]

EDUCAUSE worked with member representatives to analyze the FTC's proposed provision. Our findings formed the basis of public comments jointly submitted to the FTC by the American Council on Education (ACE), EDUCAUSE, and several other groups.[3] We determined that, in general, the proposal from the FTC strikes a reasonable balance between meeting its needs as a regulator and minimizing the reporting burden on institutions. A covered entity would only be required to report security events for which it has determined a misuse of customer information (primarily student financial aid information in the case of higher education) involving one thousand or more consumers has occurred or is reasonably likely to occur. Also, the entity would only have to report a few general elements:

- The name of and contact information for the organization
- A description of the types of information involved
- The date or date range of the event (if identified)
- A general description of the event itself

While the proposed reporting standard and structure would be workable overall, the FTC raised several questions indicating that it could conceivably take the final version of the regulation in some problematic directions from the higher education

perspective. With that in mind, EDUCAUSE and its partner associations provided a few specific points for the FTC to consider, with the goal of keeping the final provision largely within the initial parameters identified in its rulemaking notice.

The FTC clearly indicates in its rulemaking proposal that it wants to make the reports it would receive as a result of the new reporting provision publicly available, and it specifically asks if it should do so. The response from higher education associations argues that the information submitted under the proposed requirement would suit the needs of the FTC as a regulator that is trying to identify where it may need to work with a covered entity on possible compliance issues. It would be too high level, though, to provide meaningful information to students, parents, and other stakeholders and could conceivably raise anxiety among individual members of the campus community about whether their personal information might be involved. Given the likelihood that the public availability of the reports could generate undue concern among institutional stakeholders, EDUCAUSE and its partners suggested that posting all submitted reports to a national, publicly available web page might be counterproductive. If the FTC decides to proceed with such a plan, however, we asked it to consider delaying the public release of any Safeguards Rule security event report for one year from the date of submission. This would ensure that institutions have time to remediate the underlying event fully and communicate with all *affected* stakeholders before the general public release of the report in question.

The FTC also asked if the proposed requirement should explicitly exclude events involving encrypted information from

reporting, which would be consistent with the New York state regulations from which the overall revisions to the Safeguards Rule were drawn. The higher education groups noted that the reporting standard for the new requirement would generally lead to that result regardless, given that institutions would not consider encrypted data subject to misuse or likely misuse in the absence of some reasonable indication of the encryption having been compromised. Thus, we recommended that the FTC clearly state in the final regulation that entities are not required to report events involving encrypted information so long as no reasonable basis exists for thinking that the encryption involved is or is likely to be compromised.

Another key point that we raised concerns whether a covered entity should be allowed to delay reporting to the FTC if a law enforcement agency requests that it not share information about an event unless or until law enforcement gives its approval to do so. EDUCAUSE and its partner associations argued that if enacted, a Safeguards Rule reporting requirement should allow a covered entity to respect the wishes of law enforcement agencies and delay reporting at their request, given the general importance to cybersecurity of identifying and prosecuting bad actors to the extent possible. We noted, however, that the FTC could provide a way via its reporting process for a covered entity to inform the FTC that the entity is subject to such a request and provide contact information for the law enforcement agency or agencies in question. This would allow the FTC to negotiate with law enforcement as necessary about the conditions under which an entity could fulfill its normal reporting responsibilities sooner rather than later if the FTC thought a particular case warranted it.

Given the track record of the FTC concerning its rulemaking leading to the recently revised Safeguards Rule, EDUCAUSE members should assume that the FTC will adopt a Safeguards Rule reporting requirement that is similar to its proposed regulation. It is also highly likely that reports submitted under the new provision will become publicly available, although EDUCAUSE and its partners remain hopeful that the FTC will adopt a delay in providing public access to security event reports as we requested. The proposed Rule indicates that the FTC's final regulation will likely defer compliance for six months from the date of its official publication. With the early December compliance deadline for the new requirements, the FTC could issue the final version of its reporting provision in time for it to take effect at roughly the same time as the overall set of new Safeguards Rule mandates. Whether the FTC can achieve such a goal remains to be seen, but EDUCAUSE will continue to update members on any new developments with the proposed Safeguards Rule reporting requirement as they become available.

Notes

1. Jarret Cummings, **"Policy Analysis: Revised, Highly Prescriptive FTC Safeguards Rule,"** *EDUCAUSE Review,* December 2, 2021. ↩
2. Jarret Cummings, **"Cyber Incident Reporting Under the Safeguards Rule?"** *EDUCAUSE Review,* December 8, 2021. ↩
3. American Council on Education, et al., letter to the Federal Trade Commission, **"Request for Public Comment on Supplemental Notice of Proposed**

Rulemaking, 'Standards for Safeguarding Customer Information' (Safeguards Rule, 16 CFR 314, Project No. P145407), December 9, 2021—Proposed Security Event Reporting Requirement," February 7, 2021. ↩

Jarret Cummings is Senior Policy Advisor at EDUCAUSE.

Compliance, **Data Privacy**, **Federal Student Aid**

PUBLICATIONS

SP 800-171 Rev. 2

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

Documentation Topics

Date Published: February 2020 (includes updates as of January 28, 2021)

Supersedes: SP 800-171 Rev. 2 (02/21/2020)

Planning Note (4/13/2022):

The security requirements in SP 800-171 Revision 2 are available in multiple data formats. The PDF of SP 800-171 Revision 2 is the authoritative source of the CUI security requirements. If there are any discrepancies noted in the content between the CSV, XLSX, and the SP 800-171 PDF, please contact sec-cert@nist.gov and refer to the PDF as the normative source.

CUI SSP template

** There is no prescribed format or specified level of detail for system security plans. However, organizations ensure that the required information in [SP 800-171 Requirement] 3.12.4 is conveyed in those plans.

Author(s)

Ron Ross (NIST), Victoria Pillitteri (NIST), Kelley Dempsey (NIST), Mark Riddle (NARA), Gary Guissanie (IDA)

Abstract

The protection of Controlled Unclassified Information (CUI) resident in nonfederal systems and organizations is of paramount importance to federal agencies and can directly impact the ability of the federal government to successfully conduct its essential missions and functions. This publication... See full abstract

Keywords

basic security requirement; contractor systems; Controlled Unclassified Information; CUI Registry; derived security requirement; Executive Order 13556; FIPS Publication 199; FIPS Publication 200; FISMA; NIST Special Publication 800-53; nonfederal systems; security assessment; security control; security requirement; nonfederal organizations

Control Families

Access Control; Audit and Accountability; Awareness and Training; Configuration Management; Identification and Authentication; Maintenance; Media Protection; Personnel Security; Physical and Environmental Protection; System and Communications Protection; System and Information Integrity

DOCUMENTATION

Publication:

SP 800-171 Rev. 2 (DOI)

Local Download

Supplemental Material:

Security Requirements Spreadsheet (xls)

Security Requirements CSV (other)

README for CSV (txt)

CUI Plan of Action template (word)

CUI SSP template **[see Planning Note] (word)

Mapping: Cybersecurity Framework v.1.0 to SP 800-171 Rev. 2 (xls)

Other Parts of this Publication:

SP 800-171A

Related NIST Publications:

SP 800-172

Document History:

01/28/21: SP 800-171 Rev. 2 (Final)

TOPICS

Security and Privacy

audit & accountability; awareness training & education; maintenance; security controls; threats

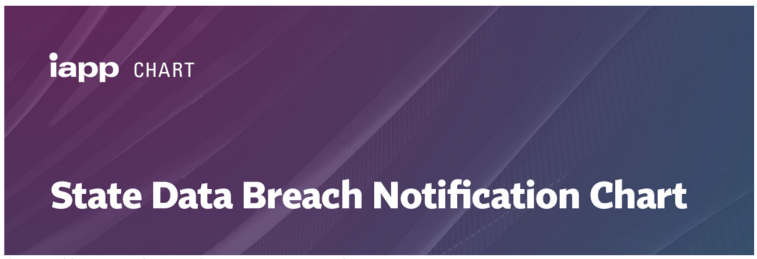
Laws and Regulations

Federal Acquisition Regulation; Federal Information Security Modernization Act

HEADQUARTERS
100 Bureau Drive
Gaithersburg, MD 20899

State Data Breach Notification Chart

Cheryl Saniuk-Heinig, CIPP/US (https://iapp.org/about/person/0011a00000vzaVGAAY)



(https://iapp.org/media/resource_center/iapp__us_state_data_breach_notification_chart.xls

Last Updated: March 2021

Click To View (XLSX)
(https://iapp.org/media/resource_center/iapp__us_state_data_breach_notification_chart.xlsx)

U.S. data breach notification laws vary across all 50 states and U.S. territories. Each law must be applied to every factual scenario to determine if a notification requirement is triggered.

territory's data breach notification law concerning entities that own, control or process personal data. The main sheet of this chart, titled "All Data – Alphabetical," lists all states followed by U.S. territories and contains:

- A hyperlink to the state's notification statute.
- The timeframe in which notification to impacted individuals is required.
- Any exceptions to notification requirements.
- If and when notification must be made to a state agency, consumer protection agency or consumer reporting agency.
- Special forms or language that must be included in the notice.
- Whether the statute provides for a private right of action.

Each column can be filtered to allow notification laws with certain features to be hidden or prioritized. As a starting point, a practitioner could filter the "Timeframe for Breach Notification" column to identify which states have the shortest notification window to further investigate the state-specific requirements. For convenience, the IAPP has also included subsequent sheets with three categories of pre-sorted data:

- Shortest notification timeframe.
- Requires attorney general notification (ranked from the lowest number of impacted individuals to highest).
- Requires consumer reporting agency notification (ranked from the lowest number of impacted individuals to highest).

This chart does not include exceptions to or additional compliance requirements with federal laws, such as the Gramm-Leach-Bliley Act or the Health Insurance Portability and Accountability Act. Additionally, an entity must determine if it owns, controls or licenses "personally identifiable information" before it can determine if the "personally identifiable information" was compromised in a "breach" (compared to a security "event" or "incident"), which will be uniquely defined by each law.

NOTE: This tool is for informational purposes only and is not legal advice. State requirements, including any recent changes, should always be verified via official sources. Requirements, if there is a security event, incident or breach, will vary depending on the

Tags: Data Loss (/tag/data-loss), Infosecurity (/tag/infosecurity), Privacy Law (/tag/privacy-law), Privacy Operations Management (/tag/privacy-operations-management), Privacy Research (/tag/privacy-research)

Pease International Tradeport, 75 Rochester Ave.
Portsmouth, NH 03801 USA • +1 603.427.9200

NATIONAL ARCHIVES

visitors, customers, and employees during the COVID-19 (coronavirus) pandemic. NARA's facilities are closed until further notice and in-person services for the public and other Federal agencies have been suspended almost entirely. All ISOO staff are teleworking remotely and we are making every effort to continue providing services whenever possible, using online and remote capabilities. ISOO's ability to serve our customers in a timely manner may be hampered by the current crisis.To ensure a more timely response to your inquiry, please contact us via email at [isoo@nara.gov / cui@nara.gov / iscap@nara.gov] We ask for your understanding and appreciate your patience. ISOO will use its blog, ISOO Overview to communicate with stakeholders on all ISOO matters. Please join for weekly posts.

Please visit the CUI blog: Controlled Unclassified Information for more information.

Established by Executive Order 13556, the Controlled Unclassified Information (CUI) program standardizes the way the Executive branch handles unclassified information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies. Learn About CUI

CUI Registry

The CUI Registry is the Government-wide online repository for Federal-level guidance regarding CUI policy and practice. However, agency personnel and contractors should first consult their agency's CUI implementing policies and program management for guidance.

Search the Registry: Go

Categories, Markings and Controls:

- Category List
- CUI Markings
- Limited Dissemination Controls
- Decontrol
- Registry Change Log

Policy and Guidance

- Executive Order 13556
- 32 CFR Part 2002 (Implementing Directive)
- CUI Marking Handbook
- CUI Notices

CUI Glossary

CUI Training

Learn about training tools developed by the Executive Agent for CUI users.

Oversight

Learn about CUI oversight requirements and tools.

CUI Resources

Learn about additional tools for handling CUI, including:

- CUI Coversheet
- CUI Marking Trifold Brochure
- CUI Audio/Photo/Video Markings Brochure
- CUI Destruction Label
- CUI Email Marking Tip
- CUI Media Labels

The U.S. National Archives and Records Administration
1-86-NARA-NARA or 1-866-272-6272

NATIONAL ARCHIVES

CUI Category: Student Records

Banner Marking for Specified Authorities: CUI//SP-STUD

Banner Marking for Basic Authorities: CUI

Category Description:	As per 20 USC 1232g, the Family Educational Rights and Privacy Act of 1974, an education record which is comprised of those records which are directly related to a student.
Category Marking:	STUD
Alternative Banner Marking for Basic Authorities:	CUI//STUD

Banner Format and Marking Notes:	Banner Format: CUI//Category Marking//Limited Dissemination Control Marking Notes: • The CUI Control Marking may consist of either the word "CONTROLLED" or the acronym "CUI", depending on agency policy. • Category marking is optional when marking Basic CUI unless required by agency policy. Example: CUI//Limited Dissemination Control. • Category Marking preceded by "SP-" is required when marking Specified CUI. Example: CUI//SP-Category Marking//Limited Dissemination Control • Whether CUI is Basic or Specified is determined by the applicable Safeguarding and/or Dissemination Authority for a given instance of CUI. • Separate multiple Category Markings by a single forward slash (/) and list Category Markings alphabetically. Example: CUI//Category Marking A/Category Marking B//Limited Dissemination Control • Category Markings for Specified CUI precede Category Markings for Basic CUI. Example: CUI//SP-Category Marking/Category Marking//Limited Dissemination Control • Separate multiple Limited Dissemination Controls by a single forward slash (/). Example: CUI//Category Marking//Limited Dissemination Control/Limited Dissemination Control • Reference 32 CFR 2002.20 , CUI Marking Handbook , Limited Dissemination Controls and individual agency policy for additional and specific marking guidelines

Notes for Safeguarding, Dissemination and Sanction Authorities:

- Whether CUI is Basic or Specified is determined by the applicable Safeguarding and/or Dissemination Authority for that CUI.
- Each "Safeguarding and/or Dissemination Authority" citation links to the statute, regulation or government-wide policy authorizing the control of that information as CUI.
- Each "Sanctions" authority links to the statute, regulation or government-wide policy that includes penalties for CUI misuse of CUI for the associated "Safeguarding and/or

Dissemination Authority" on the same line.

Safeguarding and/or Dissemination Authority	Basic or Specified	Banner Marking	Sanctions
20 USC 1232g(a)(1)(C)	Basic	CUI	
25 CFR 43.14	Basic	CUI	
25 CFR 43.22	Specified	CUI//SP-STUD	
34 CFR 99.30(a)	Basic	CUI	
34 CFR 99.31(a)(6)(ii)	Basic	CUI	
34 CFR 99.33(a)(1)	Basic	CUI	

Authority links are updated based on regular re-publication of the United States Code and Code of Federal Regulations, and the CUI Registry maintenance schedule.

Federal Student Aid
An OFFICE of the U.S. DEPARTMENT of EDUCATION

Published on https://fsapartners.ed.gov/knowledge-center/library/electronic-announcements/2020-12-18/protecting-student-information-compliance-cui-and-glba

POSTED DATE: December 18, 2020
AUTHOR: Federal Student Aid
SUBJECT: Protecting Student Information – Compliance with CUI and GLBA

As instances of data and information breaches rise, it is vital that institutions of higher education (IHEs) protect Controlled Unclassified Information (CUI) used in the administration of federal student aid programs authorized under Title IV, of the Higher Education Act, as amended[1]. FSA is finalizing the Campus Cybersecurity Program framework. A multi-year phased implementation will begin with a self-assessment of the National Institute of Standards and Technology Special Publication 800–171 Rev. 2, *Controlled Unclassified Information in Nonfederal Systems* (NIST 800–171 Rev. 2) readiness and outreach activities. We are committed to fully advancing and encouraging all postsecondary institutions implementation of NIST 800-171 controls.

This Electronic Announcement is meant to inform IHEs and their third-party servicers about upcoming activities to ensure compliance with NIST 800–171 Rev. 2. Institutions' compliance is in accordance with 32 C.F.R. Part 2002 and the federal government-wide requirement that institutions receiving CUI from the U.S. Department of Education (Department) comply with NIST 800–171 Rev. 2[2]. FSA has previously encouraged IHEs to review and adopt NIST 800–171 Rev. 2 as a security standard and to support continuing obligations under the Gramm-Leach-Bliley Act (GLBA). Since 2018, many institutions have adopted some or all of the NIST 800–171 recommended requirements. We further encourage use of NIST 800–171 Rev. 2 to help mitigate risks related to CUI.

In 2021, FSA plans to initiate a self-assessment effort to understand the IHE community's readiness to comply with NIST 800–171 Rev 2. The self-assessment effort will help the Department determine the cybersecurity posture, maturity, and future compliance of each IHE with NIST 800–171 and other cybersecurity requirements. Our intention is to partner and collaborate with IHEs, and other organizations, to enhance the resilience and maturity across IHEs by establishing a cybersecurity baseline, sharing information, and overseeing compliance with NIST 800–171 Rev. 2 and other cybersecurity requirements.

Instances of data breaches at organizations entrusted with personally identifiable information (PII) continue to proliferate and reinforce the need for the Department and IHEs to work together to combat cybersecurity threats and strengthen cybersecurity infrastructure at IHEs. Ensuring the confidentiality, security, and integrity of Title IV information depends on cooperation between the Department, IHEs, and other entities, including state grant agencies, lenders, contractors, and third-party servicers.

We expect federal student aid partners to develop, implement, and enhance information security programs with requisite controls and monitoring that supports all aspects of the administration of Title IV federal student aid programs. These security programs must encompass all systems, databases, and processes that collect, process, and distribute information — including PII — in support of applications for and receipt of Title IV student assistance.

Protecting Student Information – Next Steps

The Department looks forward to continued collaboration with IHEs to protect student data. We are committed to supporting IHEs and are working to provide additional guidelines and best practices to implement the government-wide CUI requirements, leveraging NIST security guidance. In 2021, we will post additional information to provide further information and guidance, including the cybersecurity self-assessment. In the meantime, institutions are strongly encouraged to learn more about NIST 800–171 Rev. 2 and sharing with your IT team to reduce risk surrounding CUI.

Background

The Student Aid Internet Gateway (SAIG) Enrollment Agreement entered into by each Title IV-participating institution includes a provision that the institution "[m]ust ensure that all Federal Student Aid applicant information is protected from access by or disclosure to unauthorized personnel." Institutions are reminded that under various federal and state laws and other authorities — including the HEA;[3] the *Family Educational Rights and Privacy Act* (FERPA); the *Privacy Act of 1974*, as amended; the GLBA; and state data breach and privacy laws — institutions may be responsible for losses, fines, and penalties (including criminal penalties) as a result of data breaches.

CUI is government-created or -owned information that requires safeguarding or dissemination controls consistent with applicable laws, regulations, and government-wide policies. National Archives and Records Administration's CUI rule, effective Nov. 14, 2016, 32 C.F.R. Part 2002.16, establishes that agencies must enter into an agreement with a non-executive branch entity to share CUI and require compliance with the standards set forth in the NIST 800–171 Rev. 2. The CUI program standardizes the way the Executive branch agencies handles unclassified information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and federal government-wide policies. Most data sourced from the Department and information used in the administration of Title IV programs are considered CUI.

Contact Information

If you have questions about compliance with CUI and GLBA, please contact the Cybersecurity Team at FSA_IHECyberCompliance@ed.gov or by phone at 202-245-6550.

References:

National Institute of Standards and Technology Special Publication 800-171 Rev 2 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

National Institute of Standards and Technology Special Publication 800-172 Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171 (Final Public Draft)

Federal Trade Commission Safeguards Rule

[1] 20 U.S.C. § 1070, et seq.

[2] 32 CFR § 2002.16 (5) ("Agencies should enter into agreements with any non-executive branch or foreign entity with which the agency shares or intends to share CUI.").

[3] See 20 U.S. Code § 1018b ("Any entity that maintains or transmits information under a transaction covered by this section shall maintain reasonable and appropriate administrative, technical, and physical safeguards.").

https://www.nist.gov/blogs/manufacturing-innovation-blog/what-nist-sp-800-171-and-who-needs-follow-it-0

National Institute of Standards and Technology
U.S. Department of Commerce

Manufacturing Innovation Blog

(https://www.nist.gov/blogs/manufacturing-innovation-blog)

Powered by the Manufacturing Extension Partnership (https://www.nist.gov/mep)

What Is the NIST SP 800-171 and Who Needs to Follow It?

October 8, 2019
By: Traci Spencer (https://www.nist.gov/blogs/manufacturing-innovation-blog/authors/traci-spencer)

This article originally appeared on IndustryWeek (https://www.industryweek.com/sponsored/what-nist-sp-800-171-cybersecurity-framework). Guest blog post by Traci Spencer, Grant Program Manager for TechSolve, Inc., the southwest regional partner of the Ohio MEP, part of the MEP National Network™.

Manufacturers involved in supply chains tied to government contracts can anticipate those awards bringing in additional revenue at levels that might not be possible otherwise. However, being successful in getting and keeping such work means

complying with the Federal Acquisition Regulation (FAR) and Defense Federal Acquisition Regulation Supplement (DFARS).

FAR is a set of regulations that governs all acquisitions and contracting procedures associated with the U.S. government. DFARS accompanies FAR as an addition. The Department of Defense (DoD) is the administrative body behind DFARS, but the reach of DFARS requirements extends to more than that organization.

NIST SP 800-171 is a NIST Special Publication that provides recommended requirements for protecting the confidentiality of controlled unclassified information (CUI). Defense contractors must implement the recommended requirements contained in NIST SP 800-171 to demonstrate their provision of adequate security to protect the covered defense information included in their defense contracts, as required by DFARS clause 252.204-7012. If a manufacturer is part of a DoD, General Services Administration (GSA), NASA or other federal or state agencies' supply chain, the implementation of the security requirements included in NIST SP 800-171 is a must.

How Do You Implement NIST SP 800-171?

It's understandable for manufacturers to wonder what they should do to implement NIST SP 800-171 and ultimately get in compliance with DFARS, and whether there are specialized resources available to help them achieve that milestone without preventable pitfalls. The first thing they should keep in mind is that being DFARS compliant likely involves working with a cybersecurity consultant that knows the NIST SP 800-171 requirements inside and out.

It's advisable for small manufacturers to look to their state's Manufacturing Extension Partnership (MEP) Center. Part of the MEP National Network™, a larger organization that connects them to NIST, the representatives at your local MEP Center will have a working knowledge of NIST SP 800-171 and can help companies prepare for DFARS compliance. It can be a short or long process, depending upon the complexities of a company's operating environment and information systems, but implementing NIST SP 800-171 is a necessary process for a company to protect its information.

What Does a Successful Plan Entail?

Manufacturers that want to retain their DoD, GSA, NASA and other federal and state agency contracts need to have a plan that meets the requirements of NIST SP 800-171. DFARS cybersecurity clause 252,204-7012 went into effect on Dec. 31, 2017, and deals

with processing, storing or transmitting CUI that exists on non-federal systems — such as those used by a government contractor.

One of the first steps manufacturers should take is to identify where gaps exist that prevent them from being compliant with DFARS. From that point, they can determine how to proceed.

How Should Manufacturers Start Working Toward Compliance?

The MEP National Network offers dedicated resources for manufacturers (https://www.nist.gov/mep/cybersecurity-resources-manufacturers) that need information about a company's cybersecurity posture that can help companies understand what getting compliant with DFARS actually means to them. Companies can see whether DFARS compliance applies to them and view infographics that recommend steps to take to make their factory floors more secure.

The MEP National Network also provides a particular resource that manufacturers will undoubtedly refer to again and again: the NIST Self-Assessment Handbook (https://nvlpubs.nist.gov/nistpubs/hb/2017/NIST.HB.162.pdf) (NIST Handbook 162) (https://nvlpubs.nist.gov/nistpubs/hb/2017/NIST.HB.162.pdf). It spans more than 150 pages and helps readers assess their facilities to conclude how close they are to implementing NIST SP 800-171 to help them understand how close they are to being DFARS compliant. It also helps determine where to focus efforts when making improvements to maximize the impact of each dollar spent on cybersecurity.

For example, the document features content that advises how to go about carrying out an assessment and which applicable employees to talk to regarding security requirements. Manufacturers that read through the handbook will note that each assessment question has an "alternative approach" option. It refers to the fact that manufacturers may find some requirements in NIST SP 800-171 that don't apply to them.

In that case, it's acceptable to use a different but equally effective method of maintaining security — as long as the respective manufacturers notify the correct government authorities about the changes and get approval for them.

Manufacturing plant representatives can also increase their understanding of compliance requirements by watching a webinar (https://bluejeans.com/playback/s/VZevy5gUYLnIO2QOEXrt3GVCoAJp1cWKmK210R6S1DVGeCtYmfTQo5DG7zNVVm46) that goes through some of the crucial elements of the handbook.

Complexity Shouldn't Be a Barrier

Manufacturers may initially view the cybersecurity requirements for government contracts as too complicated, especially if they have small operations.

However, using the available resources — including local MEP Centers — allows manufacturers to realize it's possible to get in compliance with DFARS, as well as stay in compliance, by implementing the NIST SP 800-171 requirements and to open possibilities for receiving financially rewarding and reputation-boosting government contracts.

A local MEP Center is an ideal resource for manufacturers to use as they start to complete a plan that details how to implement the NIST SP 800-171 cybersecurity requirements.

Each MEP Center has access to public and private sector resources that can help companies get into compliance with more confidence. Locations exist in all 50 states and Puerto Rico (https://www.nist.gov/mep/mep-national-network/connect-your-local-mep-center).

Cybersecurity (https://www.nist.gov/manufacturing-innovation-blog-categories/cybersecurity)

About the author

Traci Spencer (https://www.nist.gov/blogs/manufacturing-innovation-blog/authors/traci-spencer)

Traci Spencer is the Grant Program Manager for TechSolve, Inc., the southwest regional partner of the Ohio MEP. A member of the MEP National Network Cybersecurity Working Group, she recently completed...

Related posts

Cybersecurity for the Manufacturing Sector: Reduce Data Integrity Breaches with NIST SP 1800-10 (https://www.nist.gov/blogs/manufacturing-innovation-blog/cybersecurity-manufacturing-sector-reduce-data-integrity)
April 21, 2022

Industrial control systems (ICS) help manufacturers boost productivity, optimize efficiency and advance production lines. Historically, ICS networks were

Supporting Digital Transformation with Legacy Components (https://www.nist.gov/blogs/manufacturing-innovation-blog/supporting-digital-transformation-legacy-components)
July 20, 2021
"Information is the oil of the 21st century, and analytics is the combustion engine." – Peter Sondergaard, Senior Vice President, Gartner Research Digital

Commonly Misused Terms in Cybersecurity (https://www.nist.gov/blogs/manufacturing-innovation-blog/commonly-misused-terms-cybersecurity)
June 25, 2021
Words are hard. English is hard. How we manage to communicate anything is nigh a miracle. Sometimes I wish I was Oscar Wilde or Mark Twain or any of the other

About this blog

Manufacturing Innovation, the blog of the Manufacturing Extension Partnership (MEP) (https://www.nist.gov/mep), is a resource for manufacturers, industry experts and the public on key U.S. manufacturing topics. There are articles for those looking to dive into new strategies emerging in manufacturing as well as useful information on tools and opportunities for manufacturers.

The views presented here are those of the author and do not necessarily represent the views or policies of NIST.

If you have any questions about our blog, please contact us at mfg@nist.gov (https://www.nist.govmailto:mfg@nist.gov).

ABOUT CMMC

Frequently Asked Questions

- NOW THAT CMMC 2.0 IS PUBLISHED, WILL COMPANIES BE REQUIRED TO COMPLY WITH CMMC 1.0?
- WHEN WILL CMMC 2.0 BE REQUIRED FOR DOD CONTRACTS?
- WHY DID THE DEPARTMENT MAKE THESE CHANGES?
- HOW MUCH WILL IT COST TO IMPLEMENT CMMC 2.0?

CMMC 2.0 Briefing

- Briefing Overview (03 DEC 2021)

Current DoD Cybersecurity Efforts

- Link to Document (07 DEC 2021)

Cybersecurity is a top priority for the Department of Defense.

The Defense Industrial Base (DIB) is the target of increasingly frequent and complex cyberattacks. To protect American ingenuity and national security information, the DoD developed CMMC 2.0 to dynamically enhance DIB cybersecurity to meet evolving threats and safeguard the information that supports and enables our warfighters.

OVERVIEW OF THE CMMC PROGRAM

The Cybersecurity Maturity Model Certification (CMMC) program enhances cyber protection standards for companies in the DIB. It is designed to protect sensitive unclassified information that is shared by the Department with its contractors and subcontractors. The program incorporates a set of cybersecurity requirements into acquisition programs and provides the Department increased assurance that contractors and subcontractors are meeting these requirements.

The framework has three key features:

- **Tiered Model:** CMMC requires that companies entrusted with national security information implement cybersecurity standards at progressively advanced levels, depending on the type and sensitivity of the information. The program also sets forward the process for information flow down to subcontractors.
- **Assessment Requirement:** CMMC assessments allow the Department to verify the implementation of clear cybersecurity standards.
- **Implementation through Contracts:** Once CMMC is fully implemented, certain DoD contractors that handle sensitive unclassified DoD information will be required to achieve a particular CMMC level as a condition of contract award.

THE EVOLUTION TO CMMC 2.0

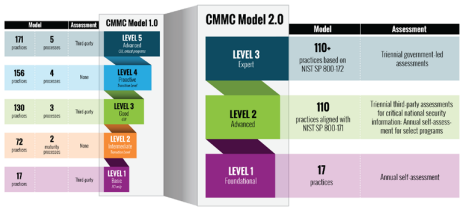
In September 2020, the DoD published an interim rule to the DFARS in the Federal Register (DFARS Case 2019-D041), which implemented the DoD's initial vision for the CMMC program ("CMMC 1.0") and outlined the basic features of the framework (tiered model, required assessments, and implementation through contracts). The interim rule became effective on November 30, 2020, establishing a five-year phase-in period.

In March 2021, the Department initiated an internal review of CMMC's implementation, informed by more than 850 public comments in response to the interim DFARS rule. This comprehensive, programmatic assessment engaged cybersecurity and acquisition leaders within DoD to refine policy and program implementation.

In November 2021, the Department announced "CMMC 2.0," an updated program structure and requirements designed to achieve the primary goals of the internal review:

- Safeguard sensitive information to enable and protect the warfighter
- Dynamically enhance DIB cybersecurity to meet evolving threats
- Ensure accountability while minimizing barriers to compliance with DoD requirements
- Contribute towards instilling a collaborative culture of cybersecurity and cyber resilience
- Maintain public trust through high professional and ethical standards

KEY FEATURES OF CMMC 2.0



With the implementation of CMMC 2.0, the Department is introducing several key changes that build on and refine the original program requirements. These are:

Streamlined Model

- ***Focused on the most critical requirements:*** Streamlines the model from 5 to 3 compliance levels
- ***Aligned with widely accepted standards:*** Uses National Institute of Standards and Technology (NIST) cybersecurity standards

Reliable Assessments

- ***Reduced assessment costs:*** Allows all companies at Level 1 (Foundational), and a subset of companies at Level 2 (Advanced) to demonstrate compliance through self-assessments
- ***Higher accountability:*** Increases oversight of professional and ethical standards of third-party assessors

Flexible Implementation

- ***Spirit of collaboration:*** Allows companies, under certain limited circumstances, to make Plans of Action & Milestones (POA&Ms) to achieve certification
- ***Added flexibility and speed:*** Allows waivers to CMMC requirements under certain limited circumstances

RULEMAKING AND TIMELINE FOR CMMC 2.0

The changes reflected in CMMC 2.0 will be implemented through the rulemaking process. Companies will be required to comply once the forthcoming rules go into effect. The Department intends to pursue rulemaking both in Part 32 of the Code of Federal Regulations (C.F.R.) as well as in the Defense Federal Acquisition Regulation Supplement (DFARS) in Part 48 of the C.F.R. Both rules will have a public comment period. Stakeholder input is critical to meeting the objectives

of the CMMC program, and the Department will actively seek opportunities to engage stakeholders as it drives towards full implementation.

While these rulemaking efforts are ongoing, the Department intends to suspend the current CMMC Piloting efforts and will not approve inclusion of a CMMC requirement in any DoD solicitation.

The Department encourages contractors to continue to enhance their cybersecurity posture during the interim period while the rulemaking is underway. The Department has developed Project Spectrum to help DIB companies assess their cyber readiness and begin adopting sound cybersecurity practices.

The DoD is exploring opportunities to provide incentives for contractors who voluntarily obtain a CMMC certification in the interim period. Additional information will be provided as it becomes available.

CONTACT US

Please provide any questions or comments utilizing the contact form.

NAME

Please enter your name

EMAIL

Please enter your email address

SUBJECT

Technical Issue with the Website

MESSAGE

Please include a detailed message

Send Email

OUSD A&S Offices

Military Services Links

Acquisition & Sustainment

Office of the Assistant Secretary of Defense for Acquisition

Office of the Assistant Secretary of Defense for Sustainment

Office of the Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs

Office of the Deputy Assistant Secretary of Defense for Industrial Policy

Office of the Executive Director for Special Access Program Central Office

Office of the Executive Director for International Cooperation

Army Acquisition

Army Sustainment

Army IE&E

Navy Acquisition

Navy Sustainment

Navy EI&E

Air Force Acquisition

Air Force Sustainment

Air Force EI&E

Resources

Accessibility | Section 508

Freedom of Information Act

DoD No FEAR Act

Plain Writing Act

Defense Strategic Plan

National Defense Strategy

USA.gov

Web Policy

External Link Disclaimer

DoD Links

US Department of Defense

USD Chief Management Office

USD Research & Engineering

USD Policy

USD Comptroller

USD Personnel & Readiness

USD Intelligence

DoD CIO

DoD Inspector General

[SUMMARY STATEMENT OF HELEN NORRIS]

Cybersecurity presents numerous challenges to the higher education community and our students, faculty, patients and staff. Universities manage complex environments and sensitive data, and need to defend against threats in the form of ransomware, hacking, phishing and social engineering. This presents numerous challenges as outlined below:

- The cost of protecting our universities against cybersecurity threats is very high;
- The threat landscape is complex and ever-changing and the tools needed to manage threats are constantly evolving;
- Ransomware incidents or breaches are disruptive and expensive;
- We have a complex regulatory environment that introduces additional complexity.

Universities protect their students and communities from these threats by:

- Utilizing sophisticated technical tools to protect our systems and networks;
- Educating our communities to be on the alert for cybersecurity risks;
- Working together to share information and best practices;
- Working with Federal agencies to stay up-to-date with new threats; and
- Preparing for the worst by preparing and exercising incident response plans.

In summary, it is important for universities to take a multi-layered approach to managing cybersecurity risks.

The CHAIR. Thank you all for your really excellent testimony this morning. We appreciate it. We will now begin a round of 5 minute questions, and I ask my colleagues to keep track of the clock and try and stay within those 5 minutes.

During the COVID–19 pandemic, we have really seen a significant increase in cyber-attacks, particularly ransomware attacks on critical infrastructure here in the U.S. And those attacks are increasingly professionalized, and oftentimes they are either sponsored or supported by foreign actors like China or Iran or Russia.

A cyber-attack, as we have talked about, on health care or education, can have a devastating impact on safety and well-being of patients and students and communities. So I want to start with this basic question, Mr. Corman. What is driving this increase in cyber-attacks and how can we better prevent and monitor them?

Mr. CORMAN. I will try to be brief, but there is more detail in the written testimony. But for now, there has really been a ransomware revolution. It used to be that Dillinger quote, why do you rob banks? That is where the money is. And most attacker adversary focus on the Fortune 100 or Fortune 500 for funds, for things that could be sold, intellectual property.

The revolution here both fueled by Bitcoin making the payments easy, but more importantly, the unavailability of whatever is important to you can be monetized for the adversary. So everyone and anyone is a target because you are in business or you are a health care institution or a university or an educational foundation, you need to function. So that unavailability became universally monetizable.

The other problem is you—when you get away with something, you keep doing it. And when you are rewarded with financial pay-

ment, you keep doing it. So we funded their R&D to come back at us harder and harder to the point where something that may have been manageable and deterrable is now nearly unstoppable.

It is a business model, some ransomware as a service with highly professionalized multi-party coordination. So we have a fairly significant problem where their bold actions went unchecked long enough and things that used to be off limits, like designated critical infrastructure—a cyber-attack on designated critical infrastructure is technically an act of war when perpetrated by a nation state.

The state tolerated and sometimes state directed, have flirted up to and across lines that we need to reestablish. That is more than just the job of Congress here, but we have allowed and tolerated the intolerable. And unless we do significant things both against the adversaries and to shore up minimum hygiene for the defenders, we should expect more of this.

The CHAIR. Anybody else want to add to that at this point. Okay. Well, I think that was pretty clear. And I appreciate that input. Let me go to this, we have seen cyber-attacks target hospitals across the country. From the largest to the smallest health care system, these attacks have really undermined the care for tens of thousands of patients in my state alone but more across the country.

Protecting patients from cyber-attacks requires significant investment in both technology and expert staff by hospitals and other facilities. How can the Federal Government help to strengthen cybersecurity across the health care sector, including actually for our rural or low income communities that have a lot fewer resources? Mr. Corman If you want to start with that, and we will go from there.

Mr. CORMAN. I am sure Denise will add. I call these organizations target rich, but cyber poor. They lack the resources to do minimum hygiene. There are significant Federal, available Federal services, and I added more while I was at CISA.

There is a free cyber hygiene scanning service that can assess your remote attack surface and tell you if you have vulnerabilities. I think one of the big challenges is we don't have sufficient reach to these cyber poor. They don't participate. They don't have CISOs yet. They don't participate in ISACs or information sharing groups. They don't know what CISA is or who is who in the pantheon of the Federal Government and when to work with HHS versus CISA versus someone else.

We have an awareness and adoption gap, but once we do engage them, I have tried to find fit for purpose things that can meet them where they are at their current skill level with empathy and give them a crawl, walk, run.

The CHAIR. Ms. Norris, maybe you can talk to us about what the Federal Government can do with the higher education within them to help support under-resourced institutions to secure their IT systems.

Ms. NORRIS. Thank you. I do agree that expanding the tools that are offered by organizations, by agencies like CISA and the outreach to those more under-resourced universities and colleges

would be excellent. In addition, perhaps we could see more tools that are more focused on higher education through agencies like CISA.

For example, the FBI has the campus security program and rolling that out, more awareness of that could be helpful. I also think that for institutions that are, have fewer resources, simplifying the regulatory environment is extremely critical, too, so that they can point their limited resources in the most effective ways.

It would also be helpful if there were some solutions to address the lack of affordability of cyber insurance for under-resourced universities. Actually, for everyone. The cost of cyber insurance and the availability is a problem, is a challenge for all of us, but it hits under-resourced institutions much more—in a much more impactful way.

Finally, it is something that we do and that we could hopefully get more engagement at the Federal level, I have heard some of the other witnesses talk about this, using Federal work study programs. We have had great success in bringing our students into our cybersecurity practice.

More engagement of our students in our universities can benefit all of us. And I know that I myself at Chapman and at other universities have made great use of that work study, for example, to help fund student engagement in this area.

The CHAIR. Thank you very much.

Senator Cassidy.

Senator CASSIDY. I am going to defer to my colleague, Senator Tuberville.

[Technical problems.]

Senator TUBERVILLE. There we go. Thank you very much. Thanks for being here today. This is a great topic. I come from education, and we are behind in a lot of things, and this is one that is dear to my heart. I just had a son graduate from college in cyber and I was shocked how many people tried to hire him because we have a huge shortage.

I was a little skeptical four or 5 years ago, really 6 years ago, he was on the 6-year plan of him getting involved in this. But my goodness, we have overlooked this problem. It is going to get worse and worse if we don't address it, especially on the state and in the higher education levels.

But Mr. McLaughlin, what can we do to encourage our younger kids, and how—what kind of programs can we put into our elementary schools to enhance young people to really get involved? They are all into video games and all that. That is totally different. I mean, this is something we have got to get them involved in.

Ms. MCLAUGHLIN. I think that is a wonderful question, Senator. There are all kinds of opportunities to bring students in early. And I think that this becomes part of creating a culture of cybersecurity and cyber safety in schools.

First off, we don't necessarily train students like we do for other safety issues from early on. We all know look both ways before you cross the street, put your seatbelt on when you get in the car. But

those kind of integrated messages about cyber safety need to be built into the messaging that students get.

On top of that, we have opportunities to build a pipeline of students who want to grow into these kind of professions later on by involving them and offering them opportunities like cybersecurity camps, cybersecurity courses.

I want to point out, it is really important that computer courses include cybersecurity as a pathway and are focused on actually how the technology works, not how to type, which has become a challenge in some spaces—lack consistency in what is offered.

Then there are some wonderful competitions that actually are offered at the Federal level for students in K–12 education and in higher education on what can they do to prevent hacking and demonstrating their skills.

Involving students and participating in that is really critical for evolving that incoming workforce and having opportunities to work in those spaces once they get to higher education, whether they are at a community college or a university.

It is a really great opportunity when we can fund, as Ms. Norris was mentioning, security operations centers and opportunities for students to develop their skills.

Senator TUBERVILLE. Thank you. In Huntsville, Alabama, we have got a new school that started over the last few years, and it is called the Alabama School of Cyber. And what they do—this is from 9th to 12th grade.

They take the top students from all over the state, rural, urban, and they bring them to Huntsville, and they train them in cyber. And of course, Huntsville is a missile defense agency, NASA, 600 defense contractors, huge. FBI is moving all of their cyber security to Huntsville, and they need more people.

They see upfront front that they are going to need this. Do we need to start doing something like this, Ms. Norris? Can you visit with me on that? All states?

Ms. NORRIS. One thing I would like to just add to what Ms. McLachlin said is that, and I heard Chair Murray refer in her comments to the digital divide. So I think as we want to bring more and more students, both from K–12 and higher education into cybersecurity, we need to make sure we continue to address that digital divide.

I think in terms of what you just described at Huntsville, we do see centers of security excellence, whether it is at the Federal level or a corporate level across different states. But I think in this new working world where people are working from everywhere, we probably have to think about ways that we can infuse security into a more globally diverse workforce, or nationally diverse workforce, as well as centers where cybersecurity is physically located. And that is one of the challenges that we have.

Senator TUBERVILLE. Yes. It takes a special person to get in this type of field. And, I would like to see in the future our higher educational institutions that accept state and Federal funding get into cyber more. I mean, we are going to need that. I mean, it is National Security.

When we are 400,000 or 500,000 short in people to do these jobs this world is getting more dangerous as we speak in terms of just anything that people can do to us, our water systems, our grids, and all those things over the years, so. Thank you all for being here today.

This will be a great hearing. And again, we are pulling for everybody to start understanding where we are at and why we are at—why we are at this spot, and we need to get better. So thank you very much. Thank you. Thank you, Senator Cassidy.

The CHAIR. Thank you.

Senator Baldwin.

Senator BALDWIN. Thank you, Madam Chair. And thank you, Senator Cassidy, for jointly bringing our attention to this. I recently helped to introduce the bipartisan Protecting and Transforming Cyber Health Care, or Patch Act, with my colleague, Senator Cassidy.

This legislation is aimed at helping protect patients from ransomware by implementing critical cybersecurity requirements for device manufacturers. And it would allow manufacturers to develop and maintain processes to update and patch devices throughout the life cycle.

Mr. Corman, you anticipated my first question in your testimony when you were talking and in your answer to a previous question when you were talking about the significant amount of research that shows how ransomware attacks constrain hospitals and ICUs, etcetera, leading to excess deaths.

I want to take my question in a slightly different direction, because while I am really proud to sponsor this legislation, it always helps me to get a more granular view of what devices are at risk of being hacked or being manipulated. You showed us a pacemaker. You talked about insulin pumps.

I am curious to know whether part of our strategy might be to make smart devices into dumb devices. We famously have a colleague on the Democratic side of the aisle who uses his flip phone just because it is safer than are iPhones and Androids.

But what about diagnostic and treatment devices in hospitals? Can they be manipulated? What about—anyways, open that up and give us some more granular examples and whether bringing some of those offline might be actually more helpful to patient, good patient outcomes.

Mr. CORMAN. I appreciate the question. In the Patch Act, I should mention as I prepared my remarks, I called some of the worst victims during the pandemic and said, what are your top three to five things you would want Congress to know? And one of them, one of the biggest victims, said, all five of my top five are, I need the Patch Act.

His point was, they never want what happened to them to ever happen again. And as they have taken a much closer look at their attack surface and their exposures, it is the unsupported software, the hardcoded passwords, the supply chain of devices, whether they be medical or just normal technology.

He can't defend that indefensible kingdom, so he wanted me to express his, I think he said I am dying of thirst and that is the water I need to wear. To your more specific question, pretty much all technologies, even 5 years ago I want to mark Thursday was the 5-year anniversary of WannaCry, the most devastating attack on health care in the world at the time and mostly hit the UK.

I remember it because we were also issuing our report to Congress for our 405c on the same day and it got delayed by 3 weeks. In that, we pointed out that a typical medical technology has over 1,000 known vulnerabilities or CVEs, and it only takes one. During the pandemic, we saw even different types of technologies that could bring down either patient care in an acute sense.

One was a radiation delivery machine that had a heavy dependance on the cloud. So you had this incredible multimillion dollar, expensive piece of gear that does its function but can't calculate how and where to precisely deliver radiation. So for several weeks, you could not deliver time sensitive cancer treatment. So the Internet of Medical Things is going to be everywhere.

It is our electronic medical records. I try to focus people in a practical sense, moving more quickly to some of the things that later in my testimony, these pragmatic security steps, these are the most dangerous practices. Instead of just referring to best practices, I got CISA to publish something called *cisa.gov bad practices*.

There are currently three, I think there is about to be a fourth, but these are the use of unsupported and end of life software in service of national critical functions and critical infrastructure is dangerous, especially egregious for internet facing. So I try to focus these target rich, cyber poor on their internet attack, surface the things reachable from the outside.

I look for things like unsupported software, hardcoded fixed passwords, and that is really the place to start. This should start to become the definition of negligence.

Senator BALDWIN. Thank you. I fear I am not going to get a full, another question in, but let me just plant a seed. I have some real concern about the third party apps that aren't covered by HIPAA and how we go about striking the right balance between access to data and efforts to protect innovation and security.

Ms. Anderson, I was going to ask you to elaborate on that. I am already out of time, and our Chair has cautioned not to exceed the time. So maybe we will get a second round, or I will submit it for the record afterwards.

The CHAIR. Okay. Thank you very.

Senator CASSIDY. I will let Senator Braun go in my place right now.

Senator BRAUN. Thank you. Thank you, Madam Chair. What I have heard most about not only on cybersecurity, but across the spectrum of workforce and enterprise is, how do we train individuals to actually be ready to take on the new landscape of jobs out there?

Running a company in a very low unemployment area prior to when I got here, I was shocked at how little is being done in the, let's say, middle school through high school time, guidance in di-

recting so many students, and a lot of times with parents okay with it, but into areas that—you are not necessarily going to benefit with a 4-year degree if it hasn't been guided well.

Half the kids that pursue it don't end up with the degree, have got time lost, and debt incurred. We need to do better. And in cybersecurity, since it is something that we talk a lot more about now than we did 10 years ago when I was actually grappling with that, I think the underlying issues are the same.

My question will be for Ms. McLaughlin. Do you think that in middle school and especially high school, are we doing the things that would prepare kids for cybersecurity career? And I would like your opinion on whether a 4-year degree is necessary for the bulk of the jobs that would be in the field, because it would be instructive, because it is the same issue I hear everywhere.

I might add that a third of the kids that get a 4-year degree end up back in the basement because it was poorly guided and there is no market for it. Here at least it looks like there is a strong market for it. Tell me a little bit about whether it is working well, pre, post-secondary education, and what is needed to be successful to fill the job.

Ms. MCLAUGHLIN. All right. Well, Senator, that is a really complicated question so I will do my best. On the middle school and high school level, and now, remember, we have 50 states plus territories. They all have their own school board governance processes, so it is difficult to extrapolate across the board.

But my observation is that curriculum content to cover issues around cybersecurity and training and development of those skills is not up to speed with the threat that we face.

Now, of course, there are exceptions and there are like charter schools or magnet schools, focused schools, and programs that do exceptionally well in this area. But across the board, I would say that we struggle in this area to get consistent training and education for students in middle and high school, and also to make sure that people are aware across the board that this is a really good career opportunity.

Now, your question about the value of a 4-year degree and the educational component for cybersecurity. I think that there are actually a couple paths in the higher education space that I want to point out. There are a number of 2 year associate degree programs at community colleges, as well as 4 year university degree programs that focus on cybersecurity.

They both have their own value ads depending on the program. And I would say that the combination of the degree plus experience working in a program where you are developing actual hands on skills is extremely valuable.

The degree focus is on the theory and the application, and then the actual practice comes from that hands on work experience. Those people often don't actually make it to graduation in a 4-year program because they are getting recruited away faster than people can get through the program.

Having said that, there are a lot of people who find alternative pathways. I would say that developing skills in the U.S. Armed

Services, developing skills through training and certification programs, are also very viable paths for developing cybersecurity professionals.

Senator BRAUN. It is a complicated question and a difficult answer, and I certainly wouldn't suggest that we should commandeer it from here. That is the bailiwick, I think, of the states. It might draw your attention.

I watched with interest Sunday morning, this past weekend, and the ex-CEOs of Merck and IBM basically said exactly what I just said. And they are 15 years later and when I was grappling with it in running my own company.

I think that given the time, the cost, it is just good for the spectrum of opportunity to make sure we are not waiting to be trained solely until you get out of, I think, that most instructive period when you are in high school. Thank you.

The CHAIR. Thank you.

Senator Hassan.

Senator HASSAN. Well, thank you, Chair Murray. And thank you again to our witnesses for being here. Mr. Corman, I want to start with a question to you. You have pointed out how dangerous cyber-attacks can be to the health and safety of the public.

In your written testimony, you stated that cyber-attacks on hospitals and health care settings can lead to additional patient deaths, and that the impact is not limited to just the health care setting directly affected but also in the surrounding region.

As you know, over the past few years, ransomware has shut down several hospitals and health care settings in and around New Hampshire, including the University of Vermont Medical Center and Coos County Family Health Services. You were working remotely in New Hampshire forces at the time. Can you speak to the impact that you saw of these attacks on the health generally of Granite Staters?

Mr. CORMAN. Sure. The excess deaths were really correlated to ICU strain, irrespective of cause. The top two contributors were not cybersecurity. They were people reluctant to try to seek medical care, introducing self-delay, and then the inability to get seen in a timely manner when they did.

The question we asked is, can cybersecurity make it worse? And we were able to use data science to measure that yes, it can. Just anecdotally, many of those affected systems in our neighboring state of Vermont, a lot of those patients were redirected and absorbed in the institutions in your own state.

I just heard a very sad story yesterday of a cybersecurity professional in New Hampshire whose mother needed an ICU bed. There were none within a 50 mile radius. She had to be treated less attentively in the E.R. and subsequently passed away. Now, this is not this hack, this person who did this. It is that we have finite capacity in our systems, especially during a pandemic.

With the mass exodus of health care workers, any elective strain, preventable, avoidable strain like 4 weeks of downtime for oncology and other things—there is an incredible case study. They were very transparent about the impacts to their oncology program and how

those were pushed to surrounding states. There is only so much capacity and when we are cavalier about avoidable, preventable harm, it has consequences.

Senator HASSAN. Thank you. I want to give each of you an opportunity to drill down a little bit on something you started to discuss in response to a question from Senator Murray. The Department of Health and Human Services, the Department of Education, CISA make more—make many affordable and often free cybersecurity resources available to the health care and education sectors.

However, as you discussed, smaller health care settings and school districts that would benefit most arguably from these resources are often just unaware that the resources exist and what the benefits are. So to each of you, in your experience, how effective is the outreach from the Federal Government to smaller entities?

I am really asking about the Federal Government's outreach and how we can improve that outreach so that these smaller entities really know what is out there and can actually connect and get some of this help. And why don't we start with you, and we will go right down the line, Ms. Anderson.

Ms. ANDERSON. I believe education is one of our biggest obstacles as far as the public knowing what services are out there for them to use. The Health ISAC, for example, in health care and many of the ISACs offer a lot of free services.

As I mentioned, the Sector Coordination Council also has free publications as well as we push all the CISA products and the HHS products as well. And so, I am going to use an example from financial services when I was with the financial services ISAC.

Treasury was very supportive of the financial services ISAC, and they actually proposed that as part of the checklist and the audits that were done against financial firms, that they belong to a sector ISAC or that they use products and services from the sector. And they—it was like a tsunami.

We called it a tsunami because people became aware of that and started joining the ISAC. And so there are a lot of ways I believe—I don't believe it is effective right now, but I do believe that if we can educate, that would be a huge great thing to do.

Senator HASSAN. Thank you. And we will go right down the line, and I will ask each of you to be pretty quick.

Mr. CORMAN. Very briefly. It has to be fit for purpose. The kind of information that an expert CISO in the ISAC needs is going to be much more sophisticated than someone who is brand new to this. So a lot of this target rich, cyber poor, pragmatic security suite. We do need to let them know CISA exists, how to work with the various parts of the Federal Government, and then make sure the advice we are giving is applicable.

Senator HASSAN. Right. Thank you.

Ms. MCLAUGHLIN. I think fit for purpose is a really good point. Most of our, 65 percent of our school districts have 2,500 students or less across the country. So having a person—having the person be able, who knows that there is a resource out there for them to use becomes a challenge.

I think one of the challenges, for once you get further—the further West you get is also—having somebody from MS-ISAC who is that point person for a region who can help people connect to the services that they need and understand why they need them.

Senator HASSAN. Thank you, and briefly, Ms. Norris.

Ms. NORRIS. Thank you. I would echo what my colleagues have said and encourage Federal agencies to continue to use the associations of ISACs and in higher ed groups like EDUCAUSE and also internet to get the word out.

Senator HASSAN. Great. And I will follow-up with questions on the record, because I think that we could have some more specific coordinating council just aimed at K through 12 and education sector so that they could have their own special assistance. Thank you.

The CHAIR. Thank you.

Senator Cassidy.

Senator CASSIDY. Thank you, Madam Chair. First, Mr. Corman, thank you for your endorsement of the Patch Act, doing with Senator Baldwin.

Just thank you for that. You make an incredibly compelling case. Not to make light of it, but my staff made this kind of funny sort of thing under a hack, and it shows this kind of increasing incidence from Health and Human Services of the amount of hacks that are occurring from 35 percent in 2016 to 22 percent now in terms of information breaches.

I say that because we see it coming. It has been happening. Unfortunately, none of the solutions that we are talking about today are kind of real time. They are like, let's make the investment for the future when we can see the trend, which is occurring now, both in the schools, upper and lower, as well as in the health care system. So I use that to frame the following discussion.

When I read about the poor, cyber poor and I am looking at Ms. McLaughlin and probably you, ma'am, as well, there is probably universities that are cyber poor because their resources are poor.

If there is such a shortage of people to do it, it is difficult to get someone. I think at the elementary school in which I attended. Now, the school system may have it, but not the school. But does therein lie a potential solution?

Mr. Corman, in terms of cyber vulnerabilities, what are the main differences between an on premise facility as opposed to a cloud based system?

Mr. CORMAN. Well, there is many ways to answer that. But one example——

Senator CASSIDY. Try to do it succinctly.

Mr. CORMAN. Yes. The most—the one that immediately comes to mind is Microsoft Exchange is like the most popular email server that you could use on premise and people try to deploy it, harden it, patch it, maintain it. Unfortunately, even though theoretically you could take better care of your own server, we have found that cloud hosted email servers are much better maintained——

Senator CASSIDY. Let me stop you. So if I go to my cyber poor hospital, and maybe I will ask about a cyber poor in university and school, it seems like—it may be difficult for them to get a cyber expert, but if they put it in the cloud, you would get the experience and the whatever of the experts who are doing the cloud based system. Is that a fair intuition?

Mr. CORMAN. There are efficiencies for hardening and security from outsourcing to expertise often in the cloud. It is not inherently riskier or better, but it seems to be less mistakes made——

Senator CASSIDY. Well, it seems like it is going to be inherently safer because you just have the expertise which is concentrated in wherever the person wishes to live, as opposed to kind of walking around to your neighborhood and doing it if you live in a small, rural neighborhood.

Mr. CORMAN. One of the top ways to reduce risk is to reduce complexity. So it is not always defending indefensible things, it is having more defensible, simpler infrastructure.

Senator CASSIDY. What is a relative expense cloud based versus a premise based system?

Mr. CORMAN. It will vary, but one idea I did suggest during my time at CISA is that we subsidize and fund that migration into cloud hosted, more secured, better maintained infrastructure.

Senator CASSIDY. Just like we once gave increased reimbursement on Medicare for people to adopt an EHR, a paradigm could be increased reimbursement for Medicare for people to migrate their system from an on premise to a cloud based?

Mr. CORMAN. Yes. A report 5 years ago had a cash for clunkers suggestion for the most dangerous and egregious technology to be modernized.

Senator CASSIDY. Yes. Now, Ms. McLaughlin, would you—is my intuition correct that we have a lot of school systems that could do better with a cloud based versus a premise based?

Ms. MCLAUGHLIN. We have a lot of school systems that already—yes, Senator. We have a lot of school systems that are already in cloud for a lot of their services. And then that leaves them with a few challenges in the cyber space, which is protecting and defending the large abundance of endpoints and ensuring that their cloud service providers are——

Senator CASSIDY. Now, just stop for 1 second. That is actually cyber hygiene, I think is the terminology as opposed to cybersecurity, correct?

Ms. MCLAUGHLIN. Yes. Well——

Senator CASSIDY. They are connected but still it is hygiene, right?

Ms. MCLAUGHLIN. Yes. And knowing what is happening and being able to respond to incidents, but also those endpoints become a gateway to potentially damage your cloud resources. So there are advantages to being in the cloud——

Senator CASSIDY. But I assuming the cloud has the ability to create cul de sacs in which somebody can't penetrate the whole because they are kind of walled off, correct?

Ms. MCLAUGHLIN. If you properly engineer your cloud services to be split up based on roles and responsibilities and that you don't have an attacker who has figured out how to traverse across the——

Senator CASSIDY. But that is the role of the cloud based service, not of the small elementary school in the rural town?

Ms. MCLAUGHLIN. Correct.

Senator CASSIDY. Yes. That is my point. It seems that—and one more thing, let me ask. It also seems, I have read about—I am out of time.

The CHAIR. You can finish. Go ahead.

Senator CASSIDY. Okay. About federated systems in which there is not a central repository of data, but rather there is a central point which then reaches out into a federation of hospitals or schools.

If you wish to look at something in aggregate, you pull it up and then you put it back. Sounds like a game that you would play in elementary school. But I assume that in a cloud based system that could similarly be allowed because you would have a wall here and a wall there and you would be federating within the system. Is that again a—Mr. Corman?

Mr. CORMAN. The cloud native innovators tend to do a much better job at distributed, immutable, ephemeral segregation, separation like you are describing. It is not guaranteed, but they seem to be doing it better.

Senator CASSIDY. Then to summarize, maybe if we want to do something relatively quickly, it would be to somehow increase funding for entities out there in order to migrate from the premise to the cloud and to put in a strong cyber hygiene program at every level. Ms. McLaughlin?

Ms. MCLAUGHLIN. I do think that would be extremely beneficial.

Senator CASSIDY. Timeline for that completion could be much shorter?

Ms. MCLAUGHLIN. I wouldn't hesitate to guess on the timeline for that completion, given the heavily distributed nature of these systems.

Senator CASSIDY. All involved is Congress to pass a law. That is very easy. So anyway, I yield. Thank you.

[Laughter.]

The CHAIR. Senator Hickenlooper.

Senator HICKENLOOPER. Thank you, Madam Chair. And thank all of you for taking the time today. So illuminating. I had to go to another meeting, but I was watching in my office. I remember when President Obama was finishing his last year, he gave a commencement address at the Air Force Academy.

I went down when I was the Governor, and we ended up having lunch together in the training room. But in that lunch, I asked him after 8 years as being President of the United States, what kept him up at night, what was the single thing that most concerned him, and he said cybersecurity, especially the way it would inter-

face with things like health care that were absolutely essential to our Country.

Which was interesting because I would come back on a trip to Israel and saw how their cybersecurity industry was so connected to their military and so connected to their universities, and that people would come out of the military, and go work in a business, then go to study and then teach.

We set up something called the National Cyber Security Center in Colorado Springs just because we have Northern Command, NORTHCOM, and Space Command, lot of intelligence there, a lot of retired military officials. And I think that building, that citadel toward cyber resiliency and awareness and training and education, just what all of you guys are doing, was one of the most rewarding things I did in the entire time I was in office.

I love, especially love the term, I am cavalry, *Iamthecavalry.org*, has got to be one of the best names. I wish we could have thought of that. Anyway, this notion of how much there is to do, and I start with Ms. Anderson. How can the Health ISAC work within the National Cyber Security Center or all the other Federal level groups to provide sector specific guidance?

Ms. ANDERSON. We do that every day, actually. We work very closely with CISA and HHS and FDA, as I mentioned in my testimony. We do have weekly meetings where we are looking at issues facing the sector and we are addressing them and trying to figure out what is the best way to handle whatever the situation is.

We are partnering very closely with them. Also, another thing during the whole Ukraine, Russia tensions, we have been part of all of the briefings that have taken place. And then we have foot stumped those messages out to our members and the public writ large about things that they need to really be paying attention to.

Senator HICKENLOOPER. Right. Good. We, like everyone, have experienced devastating attacks and especially ransomware attacks. You had 5 years of records taken from the Parkview Medical Center down in Pueblo. Last year, we—one of our universities refused to pay the ransom of $17 million ransom when they were hit by the Accellion data breach.

When colleges and universities are attacked and hospitals are being attacked with sensitive data like health information and visa status, Social Security numbers, I guess, and Ms. Norris I ask you, why is it so critical that we don't pay these ransoms?

Ms. NORRIS. I think when a ransom is paid, there is no guarantee that you are, a, going to get your data back, although there are some stats show about I think 68 percent of the time it does come back.

In addition, there is no guarantee that your data won't be published. And that is another, I think aspect of ransomware, that while the operational disruption is really critical and really impactful, there is also the threat of releasing that data out into the dark web and for it to be misused.

I think that it highlights the need to be prepared for a ransomware attack to do the things that we need to do, have a good backup, have a plan, test the plan, test the plan before you

get a ransomware attack, don't do it the first time when somebody is asking you for a ransom.

I think that is the critical way to go. It is so disruptive because it impacts the operation and the timing is always—they know when to time it, right. So they time it at a university at a time of admission or final exams so that it has the worst impact and that they will be more inclined to pay ransom.

Senator HICKENLOOPER. The only way to deal with it is be prepared. I agree completely. Mr. Corman, real quickly, just because I am almost out of time, we have a large campus of NIST in Boulder, Colorado, and they are currently in the process of updating the framework for improving critical infrastructure cybersecurity.

While this guidance is voluntary in the private sector, it is a critical resource for companies that are looking at how they can protect themselves. Given that health care has been deemed a critical infrastructure sector, how could NIST best tailor the updated guidance to meet the evolving cybersecurity needs of health care systems.

Mr. CORMAN. The NIST framework is nearly a decade now and voluntary. And the recent OIG report showed very little adoption. So it is unnecessary and insufficient.

I think you have seen some excellent work from the 405c in the joint working group in the ISAC and the Sector Coordinating Council, attempting to give that sector fit for purpose advice on how to do it. People do things when they are incentivized to do them and a decade later with voluntary, the adoption is quite low.

Even where it is, it is amongst the haves, not the have nots. I think we need carrots and sticks. If we are going to offer safe harbors, they should be tethered to an attestation about your current state of practice against such a framework tool that isn't being used, did not realize its potential.

Senator HICKENLOOPER. I couldn't agree more. Thank you. I am out of time, but I will have questions for each of you that we will filter through the appropriate channels. I yield back to the Chair.

The CHAIR. Thank you.

Senator Casey.

Senator CASEY. Chair Murray, thanks very much for having this hearing. I wanted to pose two questions to Ms. Anderson and one to Mr. Corman. Ms. Anderson, I want to start with the center that you lead.

The question is about data and tracking data. Does the center track data on negative patient outcomes that result from cyber and ransomware attacks? That is one question. No. 2 is, what are the challenges in collecting the data and how can that data be useful?

Ms. ANDERSON. We don't collect data on negative outcomes. We are actually threat—we are operational in nature, so we are looking at threats as they unfold, and we are sharing information.

We do have a saying where one person's defense becomes everyone else's offense, and we are sharing like 65,000 in 2021 actionable indicators. So real time, really true, positive indicators that help defenders put those into their system so that they can defend

against attacks. So that is the type of data that we tend to collect. And that is all members shared, by the way.

Senator CASEY. Okay. I wanted to ask you a question as well about rural health care. I represent a state that has 67 counties, but we have 48 counties that are considered rural. And rural, of course, means a lot of small towns.

But communities where there is a great distance between health care institutions and access to care and all of those challenges.

One of the big challenges, of course, is these rural hospitals and rural health centers don't have the resources that some of the big cities do, don't have the research dollars sometimes that the big universities and health systems have, so therefore they lack not only resources, but staffing to ensure that they have the requisite security in place to protect against cyber-attacks.

Just in terms of the what the center is doing, how can you and how do you help those small or medium sized health care networks?

Ms. ANDERSON. We offer many free products. And as I alluded to on the Sector Coordinating Council, their cybersecurity working group, they have put out a number of best practices publications that are freely available on the website. Just basic things that you could do with on a low budget.

There are also things that we are developing actually in the Sector Coordinating Council cybersecurity working group, a series of videos, basic cyber videos for clinicians so that they understand the aspects and impacts of cybersecurity within their practice.

There is a lot of efforts underway. I think, again, it goes back to educating people that these things do exist and that they can use them, and they don't cost anything, really.

Senator CASEY. I wanted to turn to Mr. Corman regarding a question about intelligence. I am a member of the Intelligence Committee, just became a member in 2021.

Given your background with CISA and the work you have done, what role do you envision the intelligence community more broadly playing in developing not just a cyber threat picture for the Joint Cyber Defense Collaborative, but in particular, what role do you think the intelligence community can play in developing a health care specific cyber threat picture?

Mr. CORMAN. Almost—just to be clear, two things. One, I am no longer in CISA. My public service ended in January 2. We kept this in public trust to literally be on the low side or not in the classified side. The role that we benefited from intelligence was having fit for purpose, timely, actionable decision support for the ISACs or for the practitioners that might be targeted.

We issued one of the most full throated alerts in October 2020 in advance of the U.S. Presidential election, with FBI and HHS in a pretty intense collaboration to warn of a plan to disrupt concurrent hospitals across the U.S. to sow panic. And you have now seen that covered in the Wall Street Journal and Wired in possible ties to Putin direction. So that is vital and should continue.

If there were a national agenda to prioritize the weakest or highest consequence sectors, specifically with specific programs that

maybe enhance the yield. I think the bigger issue is getting that in a timely way to the cyber poor, the rural organizations.

10 seconds—we keep talking about data. I love my privacy. I would like to be allowed to enjoy it. And most of the current regimes, like HIPAA focuses on the confidentiality of records, not the availability of patient care. So even these best practices pre-date the shift to the unavailability of health care.

Mr. CORMAN. Great. Thanks very much. Thanks, Chair Murray.

The CHAIR. Thank you. That will end our hearing today. And I really want to thank all of my colleagues, as well as our really great witnesses today. Ms. Anderson, Mr. Corman, Ms. McLaughlin, and Ms. Norris, very thoughtful conversation on a really important issue of National Security. For any Senators who wish to ask additional questions, questions for the record will be due in 10 business days, June 2nd, 5 p.m.

The Committee will next meet on Wednesday, May 25th to mark up several nominees, including Kalpana Kotegal to be a member of the Equal Employment Opportunity Commission, LaWanda Toney to be Assistant Secretary for Communications and Outreach at the Department of Education, Nasser Paydar to be Assistant Secretary for Post-Secondary Education at the Department of Education, and Rita Landgraf to be Assistant Secretary for Aging at the Department of Health and Human Services.

Thank you all again.

The Committee will stand adjourned.

QUESTIONS AND ANSWERS

RESPONSE BY DENISE ANDERSON, TO QUESTIONS FROM SENATOR BALDWIN, AND SENATOR ROSEN

SENATOR BALDWIN

I was proud to help craft the 21st Century Cures Act, which worked to address many of the interoperability concerns that we've all heard about from providers and patients. In the process, this legislation made health data much more sharable.

Question 1. Can you share any concerns that you have around the security of the health data that's gathered and used by entities not covered by HIPAA, such as third-party apps? How do we strike the right balance between access to data and efforts to protect innovation and security?

Answer 1. Senator Baldwin, thank you for your question. While there are many third-party applications covered by HIPAA, there are health applications that are provided by non-covered entities to whom individuals provide health information that can potentially be shared with others often without much transparency. I think there are three main points here:

First, while updating HIPAA is not high on the priority list given the other challenges being faced, it is time to update HIPAA. HHS has been doing what they can to provide guidance on applications and cloud, but the reality is that HIPAA is too dependent on defining covered entities and the relationships between them. Instead, HIPAA should focus on the data itself, rather than who holds/transmits it. For example, information about a patient can be shared with a covered entity and the data is protected, but if the exact, same information is shared with a non-covered entity, the data is not protected.

Second, there should be education and transparency around how data is used. There was an article published June 16th, 2022, illustrating how Facebook is receiving sensitive medical data that it can then potentially use to track patients for commercial purposes without patient knowledge:

https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites.

The Executives for Health Innovation (EHI) published a report in March 2022 that makes the case for why a robust accountability mechanism is needed to govern the use of health data held and used by health tech companies. While EHI is proposing a private-sector solution—a neutral, independently run self-regulatory program that will oversee the data use policies and procedures, the report does point out several value points:

- Defining health information broadly enough to cover all the data that reflects mental or physical well-being or health and applying to all entities that develop consumer technology and may access, hold, or use consumer health data.
- Focusing on how consumer health information is used rather than *what* information, and putting clear restrictions on the collection, disclosure, and use of consumer data.
- Shifting the burden of privacy risk off consumers and onto the companies collecting and storing consumer data. The detail, length, and density of most company privacy practices make it unrealistic and untenable for consumers to meaningfully research each technology with which they interact, nor understand the terms of use they are asked—or required—to accept before they can use each tool.
- Enabling consumers selecting health technologies to do so with less confusion and risk.
- Creating a system to receive and review consumer complaints.

https://www.ehidc.org/resources/report-case-health-data-use-accountability-outside-healthcare-system.

Finally, the security of applications and the cloud need to be continuously reinforced. While that doesn't get to the inherent problems with authorized (or at least marginally legal) sharing of individual health information, it does help address the breach scenarios. Secure software development is a hot topic and one that should be continually talked about and reinforced in every way and venue possible. Holding application developers accountable for good security practices helps to protect all information.

SENATOR ROSEN

Increasing Federal Collaboration And Resource Sharing In The Health Care And Public Health Sector: Healthcare and Public Health Sector entities are increasingly the targets of malicious cyberattacks, resulting not only in data breaches, but also driving up the cost of care and ultimately affecting patient health outcomes. Currently, Federal collaboration and information sharing between HHS and the Cybersecurity and Infrastructure Security Agency (CISA) is fragmented and limited, and many small and rural healthcare sector entities—who arguably need this Federal information sharing the most—are not aware of the many free Federal resources that are available to them. That's why I've introduced bipartisan legislation with Senator Cassidy that would require CISA to coordinate with and make resources available to Healthcare and Public Health Sector entities, including by developing products tailored to the specific needs of small and rural hospitals and health clinics. Our bipartisan bill also would authorize HHS to coordinate with CISA and private sector healthcare experts and provide training to Healthcare and Public Health Sector asset owners and operators on cybersecurity risks and mitigation.

Question 1. Ms. Anderson, I was pleased to work with the H-ISAC in developing this bipartisan bill. As the leader of a major information sharing organization, would additional Federal resources and collaboration be helpful for the H-ISAC to push out to your members?

Answer 1. Senator Rosen, thank you for your question and thank you for working with H-ISAC on this important legislation. I too believe and am a strong proponent of collaboration and while there has been good progress over the years, there is still much more we can do. I think if CISA and HHS could work with Health ISAC and the Health Sector Coordinating Council Cybersecurity Working Group together in partnership to develop and deliver products through joint webinars, workshops, products, and programs, that would be a powerful and productive way to reach those entities that may not be aware of all the resources that currently exist. As I mentioned in my testimony, many entities are not aware these resources exist and are free. The more we can push out education and broad awareness of the resources collaboratively and together as one voice, the better we can help the sector.

Public/Private collaboration during incidents or potential threats is also needed. We do have recent, good examples of collaboration, such as Health ISAC's joint product with HC3 on the geopolitical Russian threat and H-ISAC's foot-stomping of CISA's *Shields Up* messaging and information from briefings. However, the more CISA and HHS can be encouraged to approach sharing in partnership with the private sector, such as **jointly** briefing the sector on threats, situational awareness and incident response mitigations and strategies, the more powerful the impact. Again, when we can work together as one voice, the better we can help the sector.

Consideration around encouraging organizations to join the Health Sector ISAC or related ISAOs as a best practice, would be beneficial. Having a strong community of health organization participants strengthens the sector and ecosystem. Many years ago, there was some discussion around providing tax incentives for critical infrastructure organizations to join their respective sector ISACs. ISACs stood up under Presidential Decision Directive 63, are robust, valuable, sharing communities, many of which have been in existence for over two decades. Federal support in the form of incentives or grants to small organizations would go a very long way to helping these entities and the sector at large.

Finally, another area of support would involve improved regulation and control over digital currency to prevent issues like Ransomware and Digital Extortion. Crypto-currency provides for an unregulated, and anonymous money exchange that is widely used by cyber criminals to conduct nefarious activities. Crypto-currency should be highly regulated or eliminated as it is the primary mechanism fueling cyber-criminal activities and money laundering.

RESPONSE BY HELEN NORRIS, TO QUESTIONS FROM SENATOR HASSAN

SENATOR HASSAN

In her testimony, Ms. Anderson highlighted the important role that the Health Sector Coordinating Council has played in improving the cybersecurity of the health care sector. Paraphrasing from her written testimony: The Health Sector Coordinating Council serves as an official advisory council to the Federal Government with critical infrastructure protection functions distinct from the advocacy and member services roles of traditional industry associations. The education sector, however, does not have a dedicated Sector or Government Coordination Council.

Question 1. How might Sector and Government Coordinating Councils help with the critical infrastructure protection function for the education sector?

Answer 1. The coordinating council model fills an important role for sectors designated as "critical infrastructure" by the Federal Government, but that carries with it functions and responsibilities that are specific to those sectors "critical infrastructure" status. As a result, it may not be the right model for more effective DHS/CISA engagement with areas such as higher education that have national significance while not presenting the same types and levels of systemic risk as sectors like health care, transportation finance, and so forth.

With that distinction in mind, it would be worthwhile to consider how we can build on the CISA Cybersecurity Advisory Committee (CSAC) (*https://www.cisa.gov/about-cisa-cybersecurity-advisory-committee*) that was established roughly a year ago. CSAC, which includes cybersecurity leaders from a range of private and public sector organizations, serves as an official advisory body that provides the agency with broad-based input on its cybersecurity policies and programs. Given higher education's unique structure, and thus the unique cybersecurity challenges it faces, having a higher education subcommittee of the CSAC could ensure that issues and recommendations particularly relevant to colleges and universities are surfaced, both for the benefit of higher education as well as the overall cybersecurity space that the CSAC is intended to represent. Likewise, establishing such a subcommittee might provide a model for developing CISA's advisory structure so that nationally significant fields with unique structures and characteristics, which would include our colleagues in K–12, have "a seat at the table" as CISA considers how it can best work with us to advance cybersecurity nationwide.

Question 2. The Department of Health and Human Services, Department of Education, and the Cybersecurity and Infrastructure Security Agency make many affordable, and often free, cybersecurity resources available to the health care and education sectors. However, smaller health care settings and school districts that would benefit most from these resources are often not aware of these resources or their benefits.

Question 2(a). In your experience, how effective is the outreach from the Federal Government to smaller entities?

Answer 2(a). Federal agencies employ a variety of tools to reach the education sector, with electronic methods such as email and online groups being among the most effective. However, for many of us in larger institutions, we find our relationships with specific Federal agency offices and/or representatives to be more effective still. They give us an opportunity to have an interactive discussion with an agency, which allows for greater understanding and impact in the results. Unfortunately, such connections are generally not scalable, and as a result, smaller entities often feel out of the loop. In many cases, even if the Federal agencies had the capacity to reach out to every organization, the smaller entities often have limited staff with multiple responsibilities in addition to cybersecurity, adding to the communications challenges that the agencies face. Finally, the volume of information can be overwhelming for smaller entities, especially when one considers that the states are also communicating to colleges and universities.

Question 2(b). How can we improve that outreach to increase support for these entities that have the greatest need?

Answer 2(b). The Federal Government is most effective in outreach to smaller colleges when they partner with states and other organizations. For example, in California we have an organization called AICCU (*https://aiccu.edu/*) representing independent colleges, many of them smaller entities. They do an excellent job of liaising between their members and the State of California and could be effective in playing the same role with Federal entities. I would also recommend that Federal agencies target communications to non-technical leaders in smaller institutions, ensuring that the communications are clear to a non-technical audience.

In addition, a higher education-specific advisory body, as described above, would be helpful in broadening engagement. Likewise, Federal agencies should establish and maintain consistent channels of engagement and communication with national associations and organizations that support higher education cybersecurity leaders and professionals, such as EDUCAUSE and the Research and Education Networks Information Sharing and Analysis Center (REN-ISAC). The professional and operational connections that these entities sustain are often the most direct and effective ways to reach the higher education IT community at every level, from community colleges through research universities. Finally, Federal agencies could expand their methods of communication, leveraging video and social media to extend their reach given the increased prevalence of those means of engagement following the pandemic.

RESPONSE BY AMY MCLAUGHLIN, TO QUESTIONS FROM SENATOR HASSAN

SENATOR HASSAN

In her testimony, Ms. Anderson highlighted the important role that the Health Sector Coordinating Council has played in improving the cybersecurity of the health care sector. Paraphrasing from her written testimony: The Health Sector Coordinating Council serves as an official advisory council to the Federal Government with critical infrastructure protection functions distinct from the advocacy and member services roles of traditional industry associations. The education sector, however, does not have a dedicated Sector or Government Coordination Council.

Question 1. How might Sector and Government Coordinating Councils help with the critical infrastructure protection function for the education sector?

Answer 1. The Health Sector Coordinating Council is coordinated by the Cybersecurity and Infrastructure Security Agency (CISA) and offers the benefit of coordinating Federal cybersecurity resources from multiple agencies through a single working group and providing a central point of access to those resources, giving health sector organizations a single access point and reducing overlap and duplication of services.

From this perspective, a sector coordinating council for K–12 public schools could be extremely beneficial in bringing existing resources together in a single, coordinated location, identifying, and resolving gaps in resources, and reducing the development of duplicative services. Reducing the number of locations and organizations a K–12 district needs to interact with to access available resources would increase efficiency and effectiveness of those resources.

Finally, a sector specific coordinating council offers the benefit of reviewing and curating available resources from a K–12 perspective to determine if they fit the K–12 environment.

Question 2. In your written testimony, you highlighted the involvement of the Multi-State Information Sharing and Analysis Center (MS-ISAC) in supporting cybersecurity in K–12 public schools.

Question 2(a). How effectively is the MS-ISAC serving the needs of K–12 schools?

Answer 2 & 2(a). The K–12 membership in MS-ISAC has grown steadily and currently represents over 2,000 schools and districts nationally and about one fifth of the organization's membership.[1] MS-ISAC provides a valuable range of services that support the needs of K–12 schools, including:

- Malicious Domain Blocking and Reporting (MDBR)—a free service that blocks students and staff from accessing known bad websites
- Access to MS-ISAC's 4x7x365 Security Operations Center (SOC)
- Training resources including: MS-ISAC Cybersecurity Awareness Month Poster Contest for Students and Kid Safe Online Activity Book[2]

MS-ISAC actively partners with COSN and other K–12 organizations to connect with school districts, offer training and build access to the resources that support K–12 organizations. They continue to improve and expand their effectiveness in supporting K–12 schools.

One area where MS-ISAC's effectiveness has been limited is in their ability to consistently offer Security Operations Center services in a timely manner because of the rapid increase in need for SOC services caused by the increase in cyberattacks against MS-ISAC members. This impacts all MS-ISAC members, including K–12 members and is why we support increasing funding for the MS-ISAC SOC and opportunities to help MS-ISAC in staffing an expanded SOC.

Question 2(b). Do you believe that a dedicated K–12 ISAC would be beneficial?

Answer 2(b). MS-ISAC has spent significant time building relationships with K–12 schools, districts and partner organizations that developing a separate dedicated K–12 ISAC at this point may be more disruptive than helpful. Supporting and funding a K–12 specific segment of MS-ISAC would be extremely beneficial in providing a way for MS-ISAC to customize services and information specifically for the K–12 environment. For example, MS-ISAC regularly releases security advisories that are available free to all members. However, the advisories are targeted to a generic State, Local, Tribal and Territorial Government (SLTT) audience and can be difficult for the K–12 practitioner to translate into actionable activities necessary in the K–12 environment.

Question 3. The Department of Health and Human Services, Department of Education, and the Cybersecurity and Infrastructure Security Agency make many affordable, and often free, cybersecurity resources available to the health care and education sectors. However, smaller health care settings and school districts that would benefit most from these resources are often not aware of these resources or their benefits or they lack the trained personnel required to use them.

Question 3(a). In your experience, how effective is the outreach from the Federal Government to smaller entities?

Answer 3 & 3(a). Outreach from the Federal Government to smaller entities is generally less effective than it could be, for several reasons.

First, Federal Government agencies often expect or assume that there is an individual dedicated to the cybersecurity in place at each organization which is an inaccurate assumption. In smaller entities, time for cybersecurity functions competes with daily technical support and customer service, and in the smallest entities, with teaching and administration of the school. This is especially true in rural and frontier schools and districts, where not only are staff expected to take on myriad responsibilities, they are also hampered by the lack of cybersecurity skills in the local community.

Second, programs to fund additional technologies and support often come with administrative overhead and reporting requirements that are too intensive for small K–12 entities to absorb into their workload, so those programs remain unused by the groups that need them most.

---

[1] *https://www.cisecurity.org/ms—isac/k-12—text—Membership—20is—20open—20to—20all—2C—20and—20private—20sector—20partners.*

[2] Ibid.

Third, many programs developed by Federal agencies offer one-time grant funding for improvements, for example offering one-time funding for cybersecurity implementation, but don't support the ongoing costs post-implementation and/or require ongoing reporting even beyond the lifetime of the grant. This approach adds financial burden to small K–12 entities that they are unable to absorb the costs into their budgets.

Building the capacity of the Department of Education's Privacy Technical Assistance Center to help schools address their cybersecurity needs could be particularly helpful for the smallest and most resource limited school districts.

Question 3(b). How can we improve that outreach to increase support for these entities that have the greatest need?

Answer 3(b). Outreach to K–12 entities that have the greatest need can be improved by:

- Expanding K–12 access to cybersecurity resources through existing Federal programs, such as E-Rate, that are already widely used by K–12 schools and districts. In 2021, CoSN filed a petition with the FCC urging the agency to make cybersecurity costs eligible for E-rate Category 2 support.[3] The FCC has not yet published a request for comments seeking public input about the ideas featured in the CoSN petition, including modernizing the E-rate's "firewall" definition.
- Utilizing the forthcoming results of the CISA study on cybersecurity in K–12 education to develop a coordinated approach to offering cybersecurity resources that scale to fit small entities and are easy to access, and/or provide centrally funded and offered services that expand the cybersecurity capability of small entities. For example, providing the MS-ISAC Albert Network Monitoring and Management service to small entities free of charge.
- Providing funding to community college and university cybersecurity programs that operate security operations centers that offer low-cost cybersecurity monitoring and incident response services to K–12 schools and districts and serve as a training ground for new cybersecurity professionals.

[Whereupon, at 11:28 a.m., the hearing was adjourned.]

○

[3] *http://d31hzlhk6di2h5.cloudfront.net/20190903/cc/f3/72/41/228e09116606c764f2d2f2c4/CoSN-Cat-Two-Filing-Final-2019.pdf.*