S. Hrg. 118–161

IMPROVING FEDERAL COLLABORATION TO PROTECT OUR K–12 SCHOOLS FROM CYBERATTACKS

FIELD ROUNDTABLE

BEFORE THE

SUBCOMMITTEE ON
EMERGING THREATS AND SPENDING
OVERSIGHT

OF THE

COMMITTEE ON
HOMELAND SECURITY AND
GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

ONE HUNDRED EIGHTEENTH CONGRESS

FIRST SESSION

AUGUST 21, 2023

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

Printed for the use of the
Committee on Homeland Security and Governmental Affairs

U.S. GOVERNMENT PUBLISHING OFFICE
53–993 PDF WASHINGTON : 2023

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

GARY C. PETERS, Michigan, *Chairman*

THOMAS R. CARPER, Delaware	RAND PAUL, Kentucky
MAGGIE HASSAN, New Hampshire	RON JOHNSON, Wisconsin
KYRSTEN SINEMA, Arizona	JAMES LANKFORD, Oklahoma
JACKY ROSEN, Nevada	MITT ROMNEY, Utah
ALEX PADILLA, California	RICK SCOTT, Florida
JON OSSOFF, Georgia	JOSH HAWLEY, Missouri
RICHARD BLUMENTHAL, Connecticut	ROGER MARSHALL, Kansas

DAVID M. WEINBERG, *Staff Director*
ZACHARY I. SCHRAM, *Chief Counsel*
WILLIAM E. HENDERSON III, *Minority Staff Director*
LAURA W. KILBRIDE, *Chief Clerk*
ASHLEY A. GONZALEZ, *Hearing Clerk*

SUBCOMMITTEE ON EMERGING THREATS AND SPENDING OVERSIGHT

MAGGIE HASSAN, New Hampshire, *Chairman*

KYRSTEN SINEMA, Arizona	MITT ROMNEY, Utah
JACKY ROSEN, Nevada	JAMES LANKFORD, Oklahoma
JON OSSOFF, Georgia	RICK SCOTT, Florida

JASON M. YANUSSI, *Staff Director*
JILLIAN R. JOYCE, *Professionsal Staff Member*
SCOTT MACLEAN RICHARDSON, *Minority Staff Director*
JOHN A. POULSON, *Minority Professional Staff Member*
KATE KIELCESKI, *Chief Clerk*

CONTENTS

WITNESSES

MONDAY, AUGUST 21, 2023

ALPHABETICAL LIST OF WITNESSES

IMPROVING FEDERAL COLLABORATION TO PROTECT OUR K–12 SCHOOLS FROM CYBERATTACKS

MONDAY, AUGUST 21, 2023

U.S. SENATE,
SUBCOMMITTEE ON EMERGING THREATS AND SPENDING OVERSIGHT,
OF THE COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS,
Washington, DC.

The Subcommittee met, pursuant to notice, at 11:00 a.m., St. Anselm's College, The New Hampshire Institute of Politics, 100 St. Anselm Drive, Hon. Maggie Hassan, Chairwoman of the Subcommittee, presiding.

Present: Senators Hassan [presiding].

OPENING STATEMENT OF SENATOR HASSAN

Senator HASSAN. This hearing will come to order.

Good morning, everybody. The Subcommittee on Emerging Threats and Spending Oversight (ETSO) of the United States Senate Committee on Homeland Security and Governmental Affairs (HSGAC) is here today to examine the coordination efforts of Federal agencies, State and local governments, and nongovernment entities to improve the cybersecurity of our K–12 schools.

As Chair, I am pleased to bring the work of the Subcommittee on cybersecurity home to the Granite State. On that note, I would like to take a moment to recognize the New Hampshire Institute of Politics at St. Anselm's College for hosting us today. Thank you to everyone here, the staff who made this event possible.

Additionally, while Ranking Member Mitt Romney could not be with us today, I would like to thank him for his cooperation in holding this hearing, and thank his staff for the work that they have done to help organize today's event.

Now on to today's topic. As we prepare for the new school year, it is an important time to take a look at the cybersecurity of our school systems and see what can be done to increase their security and their resiliency.

Criminals and criminal organizations continue to target our K–12 schools with disruptive cyberattacks. We have seen cyberattacks on schools all across the country, including right here in New Hampshire. For example, in May, the Nashua School District experienced a significant cyberattack which took their systems offline. Across the country, according to one report, K–12 schools

publicly reported 166 cybersecurity incidents during calendar year 2021. This includes 62 ransomware incidents, which has quickly become the most common type of cybersecurity incident for K–12 schools.

However, the actual number of cybersecurity attacks is likely significantly higher than what is publicly reported because schools, and other victims of cyberattacks, too, fear the consequences of reporting cybersecurity incidents. By one estimate, the true number of incidents may be 10 to 20 times higher than the publicly reported number.

Regardless of the actual number of attacks, though, these attacks disrupt student learning and can take schools months to recover from. These attacks are not just disruptive; they are also costly. Restoring computers and networks after a cyberattack often costs the school and community over a million dollars.

Additionally, digital criminals who penetrate school systems sometimes steal sensitive information about students. In addition to holding access to computer systems hostage, also ransom the private information for money, threatening our children's privacy.

The more positive news, though, is that while cyberattacks continue to threaten our schools, Federal, State, and local governments have taken steps to combat these threats. For example, over the last few years, my colleagues and I worked to pass into law a State and local cybersecurity grant program (SLCGP) and to create the position of cybersecurity coordinator in every State.

Just 2 weeks ago, the White House announced new initiatives by Federal agencies and the private sector to protect K–12 schools from cyberattacks. One of these initiatives is something that I pushed for, the creation of a government coordinating council to focus on K–12 cybersecurity. This council will coordinate activities and policies among Federal, State, and local governments in order to improve the cyber resiliency of our schools.

In Congress, we have provided resources to Federal agencies like the Secret Service and Cybersecurity and Infrastructure Security Agency (CISA), to support the cybersecurity of State and local governments, including public schools.

Today we will hear from a panel of experts who have all played different roles in improving K–12 cybersecurity in New Hampshire, representing Federal, State, and local levels of government. The panelists will discuss innovative and collaborative cybersecurity efforts among the offices and agencies charged with protecting our schools, as well as how we can continue to work together to address remaining cybersecurity challenges.

As students in New Hampshire head back to school this year, I hope that today's conversation highlights the importance of continuing to work together to improve K–12 cybersecurity and inform our communities about this critical issue.

Now on to the panel. I will introduce each panelist and ask them to provide their remarks, and then we will go into the question section of the panel discussion.

Our first panelist today is Daniel King. Mr. King serves as the chief of cybersecurity for region 1 covering New England for the Cybersecurity and Infrastructure Security Agency (CISA). Prior to his time in CISA, Mr. King was global lead for International Busi-

ness Machines (IBM) security command, and served 30 years on active duty with the United States Army.

Welcome, Mr. King, and thank you for your years of service. You are recognized for your opening remarks.

TESTIMONY OF DANIEL KING, CHIEF OF CYBERSECURITY, REGION 1 (NEW ENGLAND) CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. KING. Thank you, Madam Chair. It is a pleasure to be here today and this opportunity to participate in today's roundtable. This format lends itself to meaningful dialogue, and, for that, we are grateful for a conversation that otherwise may not occur in a more formal question and answer format.

CISA region 1 is headquartered in Boston. We have a team of 50 and 9 cybersecurity advisors joining both protective and chemical security advisors supporting the six States and 10 tribal territories and nearly 15 million citizens of New England.

CISA is very effective despite its relatively small size within Department of Homeland Security (DHS) because we live in and support the communities that we serve. We are here through fair and foul in commitment and partnership with State, local, tribal, territorial (SLTT) entities across our great nation.

CISA's regional advisors support and assist and assess organizations to reduce risk and improve security because management and prevention of threats is far, far less expensive than the alternative.

In 2023 alone, the security advisors of region 1 have engaged, assessed, and supported nearly 200 K–12 organizations across New England, and that number speaks to CISA's focus on this vital part of our community and our Nation. Each engagement, assessment, and assist visit improves awareness and opens the path to reduction of risk and improvement of resiliency. But as our schools now rely foundationally upon the Internet connective information system technologies we have as a core capability, with that dependency comes significant risk from cyber threats.

Unfortunately, and due to very narrow operating margins, our K–12 entities are clearly cyber target rich and resource poor. Criminal actors recognize how vulnerable schools are to cyberattack. To them, this is an opportunity. To us, this is a crime exploiting the innocent.

We have seen it, as you mentioned, Senator, here in New Hampshire and across New England, and it will continue until we adopt better cybersecurity practices and make defending our schools in cyberspace a public priority.

CISA is focused upon securing the nation's criminal infrastructure like K–12 by providing resources that enable the U.S.'s over 13,000 school districts to better protect and defend their students and employees against cyberattacks.

What are we doing here in region 1? Our most impactful work is before the incident, working with schools to identify, manage, and reduce risk, working to ensure that when they are hit by a cyber incident, they are prepared, have a plan, and can mitigate the impacts of the incident.

School safety and K–12 cybersecurity can be complex and often unique to the communities they serve, so our efforts must be collaborative, built upon dialogue, information sharing, and, most importantly, trust. We cannot do this without strong partnerships across Federal, State, and local levels. Perhaps this is one of the strongest examples you can see here today of all of us sitting shoulder to shoulder against this threat.

In addition to the recent DHS, Department of Education, Health and Human Services (HHS), and Department of Justice (DOJ) announcement of school safety awareness, CISA released a report that provides recommendations and resources to help K–12 schools and school districts effectively reduce their risk, an evolving disruption and damaging cybersecurity threat landscape. This report and new K–12 digital toolkit provides clear recommendations and resources to help K–12 organizations to effectively reduce their continuously evolving cyber risk.

These national efforts, along with your continued support, Senator, of the State and local cybersecurity grant program, help States, and specifically rural and local communities, to address cybersecurity risks. I would also add that New Hampshire was the very first that submitted their proposal for the grant program, and was approved.

At the regional level, we leverage impactful national investment to deliver the last mile, a rare thing from a Federal perspective, where our regional security advisors meet with and provide direct support to our local partners, specifically for K–12 regional advisors, engaged leaders, educators, and technical staff, by assisting them to recognize the importance of implementation of multifactor authentication, identification of critical systems and data to ensure that those systems are assured by backup and resilient to disruption, to implement CISA's cyber performance goals and alignment of cybersecurity plans to enlist approved guidelines and perhaps, most importantly, shape the development of plans, training, and exercises to illuminate cyberrisk and reduce impact.

Beyond providing direct services, cybersecurity advisors enable access to national-level resources such as no-cost vulnerability scanning of Internet-facing infrastructure and the ransomware vulnerability pilot, along with other programs that provide actionable early warning before an attack happens.

When a cyber incident does happen, our advisors are there with our State and local and tribal partners alongside with law enforcement at all levels to support the recovery of the victim.

In sum, CISA and its personnel in region 1 are reducing risk and improving resilience to critical infrastructure, and, yet, K–12 schools represent perhaps our most vital of all critical infrastructures.

Our schools and their students are truly our future. We work side by side with our State and local partners to reduce risk, and with your continued support, Senator, to protect this most precious resource. Thank you.

Chairman HASSAN. Thank you very much, Mr. King. Now, I would like to introduce our next panelist who joins us today also from CISA. Mr. Richard Rossi has been with the Department of Homeland Security for more than 17 years and currently serves as

the first-ever cybersecurity advisor for New Hampshire, a position he's been in for approximately 2 years.

Having led bipartisan efforts to create this important position in each State, I am very glad that you are in this role and here today, Mr. Rossi, and I am extremely grateful for your service to the Granite State.

You are now recognized for your opening remarks.

TESTIMONY OF RICHARD ROSSI, CYBERSECURITY ADVISOR—NEW HAMPSHIRE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. ROSSI. Madam Chair, thank you for convening this group today to discuss protecting K–12 schools from cyberattacks. I appreciate the opportunity to discuss the efforts of the Cybersecurity and Infrastructure Security Agency to improve the cybersecurity of K–12 schools in New Hampshire.

Over the past several years, K–12 schools and school districts have adopted advanced Internet-connected technologies and cloud resources that facilitate learning and make school more efficient and effective. This technological gain, however, is accompanied by heightened risks, and greatly increases, both in scope and complexity, the cyberattack surface a school district needs to defend.

Malicious cyber actors are targeting K–12 education organizations across the country with potentially catastrophic impacts on students, their families, teachers, and administrators.

An October 2022 report from the Government Accountability Office (GAO) found that more than 1.2 million students were affected in 2020 alone with lost learning ranging from 3 days to three weeks, and recovery time from 2 months to 9 months.

Nearly one in three U.S. school districts had been breached by the end of 2021, according to a survey by the Center of Internet Security, with incidents including student data breaches, ransomware attacks, business email compromise, data breaches involving teachers and school community members, denial of service attacks, website and social media defacement, as well as online class and school meeting invasions.

The lack of funding and investment in K–12 cybersecurity continues to work against school districts' ability to plan for, prepare against, and mitigate the effects of cyber attacks. In its 2023 annual survey, the Consortium for School Networking (CoSN), of which the New Hampshire Chief Technology Officer (CTO) Council is an affiliate, found that 66 percent of districts nationally lacked a full-time cybersecurity position, and half do not have adequate staff to integrate technology into the classroom. The same survey highlighted that just nine percent of districts spend more than 1/10th of their information technology (IT) budget on cybersecurity defense, while 48 percent of districts dedicated less than 2 percent of their IT budget to security. A full 12 percent dedicated zero budget to cybersecurity.

The scale and scope of the cybersecurity threat environment is such that no one individual or agency is equipped to address the issues on their own. As the CISA cybersecurity advisor and State coordinator assigned to New Hampshire, I enjoy tremendous col-

laborative relationships in the mission to improve K–12 cybersecurity. None of this work is done in a siloed fashion, and I want to recognize the New Hampshire Department of Information Technology (DoIT), Primex, The ATOM Group, and the U.S. Secret Service (USSS) for their steadfast partnership in these efforts.

There is a plethora of free cybersecurity resources from Federal and State government for K–12 schools, and I am confident with the collaborative construct we have developed in New Hampshire, contact from any one of these agencies brings to bear the full resources of all of us.

Within the State of New Hampshire, CISA efforts to improve K–12 cybersecurity have come in many forms. Broader communication campaigns on cybersecurity threat best practices and resources have been presented in larger forums including the New Hampshire Chief Technology Officer Council clinic which is compromised of K–12 IT directors from throughout the State, and the New Hampshire Association of School Business Officials made up of business officials and administrators from the K–12 school districts throughout New Hampshire.

Thanks to your continued support, Senator, New Hampshire K–12 school districts will also benefit from the Cybersecurity and Information Security Agency—Federal Emergency Management Agency (CISA–FEMA) jointly administered State and local cybersecurity grant program through leadership with the State Cybersecurity Planning Committee, by Commissioner Goulet, and chief information security officer Ken Weeks.

While there are common cybersecurity challenges among K–12 schools, each district is unique. That uniqueness is leveraged as an opportunity to have a one-on-one conversation with each individual K–12 IT director seeking to improve their cybersecurity posture. That provides insight to the challenges, concerns, and priorities within a given district. That insight is then leveraged by CISA to develop a tailored roadmap to improve cybersecurity and resiliency within school networks. CISA's support to improving K–12 cybersecurity in the State has come in many forms, including onsite cybersecurity and ransomware readiness assessments, assistance of policy development, tailored advice, cybersecurity training, support for cybersecurity tabletop exercises, penetration testing, continuous cyber hygiene vulnerability scanning, implementation assistance with technical controls and tools, reviewing public-facing websites for information that can be used in social engineering and fraud schemes, among other areas.

Through the cybersecurity assessment process locally, it's strongly encouraged that school district leadership attend the assessment findings outreach, and the vast majority of district administrators have done so. This format is in recognition that cybersecurity is not just the IT department's problem, but rather whole of organization business problem.

Changes in K–12 cybersecurity must come from the top. Leaders must establish and reinforce a cybersecurity culture while recognizing and actively addressing resource constraints.

I am confident the dialogue in these briefings has led to an increased awareness of the cybersecurity threat and vulnerabilities in a given district, as well as the initial development of a cyberse-

curity culture that will ultimately benefit all. This collaborative work alongside New Hampshire school districts has led to mitigation of vulnerabilities cyber threat actors leverage to conduct damaging cyberattacks.

Thank you for the opportunity to be here today, and I look forward to the roundtable discussion.

Senator HASSAN. Thank you so much.

Our third panelist today joins us from the Secret Service. Mr. Tim Benitez serves as the resident agent in charge for Manchester, New Hampshire. Resident Agent Benitez has over 24 years of law enforcement experience, and currently supervises the New Hampshire Cyber Fraud Task Force's digital forensic incident response team.

Resident Agent Benitez, you are recognized for your opening remarks. Thank you for being here.

TESTIMONY OF TIMOTHY BENITEZ, RESIDENT AGENT IN CHARGE, MANCHESTER, NH, U.S. SECRET SERVICE, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. BENITEZ. Thank you. Good morning, Senator Hassan, Members of the panel, and attendees here today. I thank you for the opportunity to discuss the ongoing efforts of the U.S. Secret Service to protect the nation's financial infrastructure.

I serve as a supervisory special agent in Manchester, New Hampshire, where I'm responsible for managing our integrated mission of physical protection and investigating cyber-enabled financial fraud.

In New Hampshire, our cyber fraud task force (CFTF), is a collaboration between the public and private sector whose mission is to prevent, detect, and mitigate complex cyber-enabled financial crimes against payment systems and critical infrastructure.

Participating State and local law enforcement, prosecutors and judges have received specialized digital forensic cyber investigation and cryptocurrency tracing training at the National Computer Forensic Institute (NCFI) in Hoover, Alabama. The Secret Service established the center in 2008 and we are grateful that Senator Hassan co-sponsored the NCFI Reauthorization Act which provides funding through 2028.

In fiscal year 2022, New Hampshire personnel have attended over 47 courses, receiving almost $300,000 in equipment. We are currently on track to match those numbers for fiscal year 2023.

There is no cost to attend the NCFI, and many courses include significant equipment issuance. For example, mobile device forensic examiner course provides $28,000 in equipment. The basic computer evidence recovery training course provides $35,000 in equipment.

The graduates of these courses return to their respective departments to investigate criminal activity and strengthen prosecution utilizing digital evidence recovery methods. While at their departments, the CFTF continues to collaborate and provide necessary resources.

The Internet Crime Complaint Center (IC3.gov), 2022 statistics reports indicates that New Hampshire is experiencing an increase in cyberattacks and cyber-enabled financial fraud schemes.

While these statistics are significant, they are underreported since many victims fail to report or are reporting to other entities.

In 2022, 1,416 New Hampshire complainants lost $29.3 million, an increase of $14 million from 2021. Nationwide, cyberfraud totaled $10.3 billion, with business email compromised totaling $2.7 billion; investment scams, $3.3 billion; tech call center scams, $1 billion; and ransomware, $35.3 million. This ransomware number does not include the business revenue lost and the significant cost of incident response and repair services.

Cyber attacks can be complex, or executed successfully by preying on individuals that are susceptible. As a world becomes increasingly digital, it is important that individuals and organizational leaders understand and mitigate cybersecurity risks utilizing both training and technological solutions.

I look forward to discussing these topics further and how law enforcement can be more impactful. Thank you.

Senator HASSAN. Thank you very much.

Now our next panelist is Mr. Denis Goulet. As Governor, I had the pleasure of appointing Mr. Goulet as Commissioner and Chief Information Officer (CIO) for the State of New Hampshire Department of Information Technology in 2015. He has since been reappointed for two additional 4-year terms by Governor Sununu.

Commissioner Goulet brings nearly 30 years of private sector IT experience to his public service. Welcome, Commissioner. You are recognized for your opening remarks.

TESTIMONY OF DENIS GOULET, COMMISSIONER AND CHIEF INFORMATION OFFICER, STATE OF NEW HAMPSHIRE DEPARTMENT OF INFORMATION TECHNOLOGY

Mr. GOULET. Thank you, Madam Chair. Thank you, first of all, from the bottom of my heart for, in 2015, trusting me with the most interesting, challenging, and rewarding job I have had in my career. Also, thank you for your leadership in the cybersecurity space.

I think it might not have been 10 minutes into my role as Commissioner for the Department of Information Technology that then Governor Hassan and her office were talking to me about cyber. We have seen that leadership move through her change to the role of Senator and now national leadership where we have our friend and colleague, Rick Rossi. Thank you very much for your leadership on that. That has been a tremendous help. I think Rick is a credit to his organization in his role in the State, and also the work on the State and local cybersecurity grant program. We are going to make sure that is a game changer in New Hampshire for K–12s and the municipalities as well.

As we walk around and do our jobs every day, we often hear from our colleagues, "Who owns cyber?" You know, it's as if it should be an organizational or a thing where, there is this centralized authority for cybersecurity. Answer is we all do. We all do.

Early in my tenure here in New Hampshire, myself and then Director of Homeland Security and Emergency Management, Perry Plummer, coined the phrase "There is no 'I' in cyber." We live that in New Hampshire. We are the live free or die State, right? You would think, oh, we are fiercely independent. In some ways, we

are. But what I found is that the ability to team on important things in New Hampshire is exceptional, and we are seeing that here in New Hampshire on cybersecurity.

You have heard it already from all of the panelists so far, the level of collaboration we have. We all have each other on speed dial. Whoever finds out first, we pull each other in.

What that is resulted in is even though there were quite a few administrative hoops to jump through to actually access the year one SLCGP, State and local cybersecurity grant program monies, New Hampshire was first in the Nation to both get plan approval as well as to accept the money.

That is great for K–12s because we are operationalizing that already in our process of rolling out the plan.

Now, when you look at that grant, it is a large amount of money by any measure, nationally, but when it comes down to each State, it is an amount that needs to be managed carefully. We cannot afford to use that money in a wasteful way. Fortunately, what has happened in our case, we already had that collaborative environment that we were working on together. The focus on our use of that money is very much on making the most of it, bringing it to the K–12s and municipalities in a way that they can leverage it, and doing it through programs versus subgrants. We are, nationally, one of the first to do it that way as well, and it is being recognized that that is the way to do it.

The other thing I want to comment on is, do I have enough money in my State budget to do everything I would like to do from a cybersecurity perspective? Do I?

Mr. WEEKS. No, sir, you don't.

Mr. GOULET. OK. Despite that, we are taking the SLCGP monies. We are allowed to use 20 percent of those for State. We are not doing that in New Hampshire. Because even though I do not have enough money, I am in better shape than the K–12s and the municipalities.

Other than a relatively small percentage that we are using to operate the program, all of that money is going down to the folks who need it the most. This is a great chance for us to all discuss how we are doing that and how we can all make each other better. Thank you.

Senator HASSAN. Thank you very much, Commissioner.

Our fifth panelist works closely with Commissioner Goulet, as you just heard, for the State of New Hampshire. Mr. Ken Weeks serves as the chief information security officer for the New Hampshire Department of Information Technology. Prior to that, Mr. Weeks spent most of his adult life as a naval officer special duty cryptology information warfare, retiring as a captain.

Mr. Weeks, welcome. Thank you for your service. You are recognized for your opening remarks.

TESTIMONY OF KENNETH WEEKS, CHIEF INFORMATION SECURITY OFFICER, STATE OF NEW HAMPSHIRE DEPARTMENT OF INFORMATION TECHNOLOGY

Mr. WEEKS. Good morning. Thank you, Chair Hassan.

It is a real pleasure to be here this morning. When I first took this job, I would been in my role for a little over a year now, two

very strong-willed ladies—one of whom happens to be sitting to my left—and another one named Sonja Gonzalez, on our first very meeting, said, "Hey, Ken. We appreciate how you can help and how the State will try to help us, but we do not need someone to tell us what to do. We need help actually doing it."

That resonated with me and stuck with me. I spend an awful lot of time listening and developing relationships with the New Hampshire Chief Technology Officer organization—there's members in the audience here, and Pam used to be a member of that organization—as well as the New Hampshire Municipal Association. What that did was allow us to have insight on what individual SAUs, K–12s across the State, needed. Because what we quickly found out was that if you knew one, you knew one. You did not necessarily know all. There were some commonalities, but they had very different problem sets and were going to require a very different tailored set of services to get them what they need to protect their student data, enable staff, and to, quite honestly, keep the schools open.

Those relationships have grown over time. We also, here in New Hampshire, as you very well know, ma'am, have the luxury that almost all of the school districts within New Hampshire are part of one public risk management exchange. That also allows us to leverage things that are already known through the Primex processes as far as what the needs are. Again, individually, not just generically and across the board.

The attitude that we have taken—and we will get into more detail about this in the question and answer—for both the State and local cybersecurity grant program as well as the State Homeland Security grant program, is that we want to provide additive services and go out of our way to not duplicate anything that is already available through Primex or some other means that folks already have access to.

I think that goes to Commissioner Goulet's point of trying to maximize the effectiveness of the money by ensuring there is no duplication.

The last thing that I would say, it is come up a couple of times from other panelists, but the importance of a partnership and collaboration between the Federal level, the State level, and the local level with the SAUs and those chief technology officers and those administrators directly. Routinely, Mr. Rossi, Mr. Benitez, Mr. Casey, who's in the audience and is a risk manager at Primex, and Mr. Sgro, who is the senior partner at ATOM and the chairman of the board for the newly formed Overwatch Foundation, and myself, are talking to groups of chief technology officers and local representatives, in every forum that you can imagine from the Primex annual meeting to the New Hampshire Chief Technology Officer meetings that are held quarterly, as well as the New Hampshire Municipal Association meetings. That is allowed us to very effectively team and bring all the resources from our different agencies to bear on the cybersecurity problems of New Hampshire.

Thank you very much for an opportunity to be here. I look forward to the question and answer period, ma'am.

Senator HASSAN. Thank you very much.

Our final panelist today is Ms. Pam McLeod. Ms. McLeod currently serves as chair of the Alton school board. Prior to that, she spent 19 years as an administrator in New Hampshire public schools. Most recently, she was the director of technology and chief information security officer for the Concord school district. Ms. McLeod founded the New Hampshire Chief Technology Officers' Council and the Student Privacy Alliance. Ms. McLeod, welcome. You are recognized for your opening remarks.

TESTIMONY OF PAMELA MCLEOD, CHAIR, ALTON SCHOOL BOARD

Ms. MCLEOD. Thank you. Thank you for having me. I want to echo our appreciation for all of your work on cybersecurity, Chair. It really is noticed amongst our school districts in New Hampshire.

First, I want to say I served 10 years in a small K–8 district in Alton as the director of technology before moving on to Concord. I am currently a board member in that same school district, so I really do have the perspective of our many small school districts at heart in a lot of what we do.

IT has changed a lot. Our IT leaders are not hiding in a closet. We are not boxes and wires people anymore. We have some of those working for us. But, we are collaborative. I think the thing that New Hampshire is getting noticed for around the country is really the collaboration, the grassroots efforts that we have particularly related to student data privacy.

Our student data privacy initiative——completely volunteer—has covered over 1,500 ed tech vendors since 2018, since New Hampshire's student data privacy law was passed in 2018. We work with four other States in that initiative, and we serve at least 82 percent of New Hampshire's public school students. I am not sure what the other 20 percent are doing, 18 to 20 percent. But it has been noticed around the country and has been very successful.

We appreciate the tight working relationship that we have with the State CIO and chief information security officer (CISO), with CISA, and particularly Rick Rossi. Multistate Information Sharing and Analysis Center (MS–ISAC) has been fabulous. The U.S. Secret Service, Primex, and the ATOM Group. It is that kind of collaboration that really enables us to survive when it comes to cybersecurity.

I am here to talk about what we need. Some of the things that we need are, we do not need more documents and more instructions. What we need are resources. Time and money, of course, are always the issue in schools.

I have long thought that regional cybersecurity experts—"regional" in terms of New Hampshire's regions: North Country, Lakes Region, Southeast, et cetera—who can actually go into schools and configure settings for them would be a really great advantage for schools. It would really help both schools and municipalities address the cybersecurity issues that they have.

I think having funding possibly through E-rate—and I really appreciate FCC Commissioner Rosenworcel's commitment to K–12, and potentially funding cybersecurity would be fabulous. Funding Managed Detection and Response (MDR) or Security Operations Center (SOC) services would be amazing for school districts. Really

offloading that task of watching logs, of watching intrusions off to a service would be fabulous.

As I left Concord, we had taken advantage. CISA does have a K–12 discount on SOC services with CrowdStrike, and we were just implementing that as I left Concord earlier this summer. But that really is potentially a game changer for school districts.

I think what New Hampshire has done with the grant programs has been amazing, and as they prepare to roll out YubiKeys for multi-factor authentication (MFA), .Gov in a Box, security training, really fabulous. One of my colleagues from another State, when they heard about New Hampshire's grant application, said, "Well, what my State gave me is a waiver." We really appreciate the efforts of the State in that respect.

Then I think there is a lot on the vendors. I think it is really important for our ed tech vendors not to hide security behind a paywall. I am a strong user of both Google and Microsoft's tools, but both services hide security features, which should be basic, behind a paywall. That is an important change that really needs to happen.

After watching the White House events a couple of weeks ago, fantastic to see the attention paid to K–12 cybersecurity. As I watched the vendors' offerings, I felt they were a little fluffy. I really like to give some kudos to Cloudflare, which has a really tangible offering for districts under 2,500 students.

I have no association with Cloudflare. I have never used their services. But they really stood out in terms of actually offering something to school districts.

Then I think there is a lot on the districts as well. School districts must require phish-resistant multifactor authentication. It is way past time to fight that battle. I think the State's grant program is going to help that a lot. Teachers' unions need to get on board with that particular initiative as well. School districts need to prepare with security audits. CISA will come and do some auditing for free. The ATOM Group, who is our forensic first responder through Primex, will do it at a very reasonable rate. Fantastic opportunities for districts there.

IT staffing is a huge problem. Turnover is a huge problem in K–12 with IT. I think there are practical things that can be done which may not cost a lot of money.

In my role as a school board member, we work to do market adjustments for IT staff to really make sure that everybody knows your compensation in the public sector is not going to match what you can get in the private sector. However, there is still a lot you can do to really build things up and make your staff happier.

Monetary and nonmonetary. Things like work-from-home hybrid models. Different kinds of benefits as well as some adjustments to compensation. I do not know the answer to that, but it certainly is a big issue that we have in school districts.

I guess I would leave with districts know how to employ teachers. They are really good at employing teachers. They really do not know how to compete for IT staff. Perhaps there could be some partnerships with the Federal Government and the State in terms of developing salaries, scales, and steps, other kinds of initiatives.

Denis has done a fantastic job with that at the State of New Hampshire to really maintain that staffing.

Thank you very much for having me.

Senator HASSAN. Thank you very much for that testimony. Now I am going to pose some questions to the panel. I have a number of them. My final question will be, essentially, is there anything that we did not get to that you all wanted us to get to, or anything you wanted to add to somebody else's comments?

As you are listening, if there is something that strikes you, feel free to make a note, and I will come back to give everybody a chance to add final thoughts at the end of the questions.

I want to start with a question to you, Mr. King. Cyberattacks continue to target K–12 schools across the country. According to information from two nonprofit organizations, the Multistate Information Sharing and Analysis Center and the K–12 Security Information Exchange (SIE), there have been more than 1,000 cybersecurity incidents impacting K–12 schools since 2016. This does not include incidents that are not reported publicly.

Mr. King, for school administrators and parents, how would you describe the current cybersecurity threat for K–12 schools in New Hampshire and New England?

Mr. KING. Thank you, Madam Chair. It is hard to understate how great a threat and a risk there is to schools. It is a condition of how we manage our municipalities and how we deliver education in this country that we are forced to make hard choices about how to spend a dollar for education, and as we have adopted these more increasingly advanced and convenient technologies, some of them at a complexity level that obscures risk entirely. We have certainly leveraged those technologies to navigate the impact of Coronavirus Disease 2019 (COVID–19) and successfully mitigate those impacts. Unfortunately, as we have stepped down that path, we have inherited all the risk associated with it.

Our environments for education have changed. Because of our reliance on these technologies, we have to look at a completely different understanding of risk and resiliency when it comes to utilization of these technologies within our schools.

Senator HASSAN. Thank you.

Ms. McLeod, I asked Mr. King about the cybersecurity threat landscape really so that Granite Staters can get a sense of the size and scope of the threats we are facing. I think it is also important that people understand the impacts of a cyberattack on a K–12 school system. You are on the Alton school board and you previously served as director of technology of the Concord school district and have other school district experience, so you have experience addressing cybersecurity gaps.

Can you explain how a cyberattack impacts a K–12 school? What are the consequences for school budgets, for student privacy, and for classroom time?

Ms. MCLEOD. Yes, so in Concord, we were, I consider, fortunate to be breached early in 2016. That really enforced and influenced our approach to cybersecurity after that. We had a breach of all of our staff W–2's. Every single staff member in the district has had their data privacy compromised. Many of those staff members were, for instance, refugee students who were working as summer

custodians for the district. Not just adults, but also student employees as well.

It is devastating. It really takes all of the district's time and resources to handle an attack like that for a period of 2 to 4 weeks. It really is all-consuming. In the meantime, you are trying to keep a whole infrastructure going. You are trying to run a school district. You are trying to keep all of your other business going. You are already stretched very thin. It really is devastating.

Senator HASSAN. In at least some cases can interrupt student learning time, too.

Ms. MCLEOD. Absolutely. Yes.

Senator HASSAN. In terms of school budgets, do you remember what the impact was on Concord back in 2016, or do you have examples to share?

Ms. MCLEOD. I do not remember what the impact was. I am sorry, I did not come with the number.

Senator HASSAN. That is all right.

Ms. MCLEOD. I know that many school districts are reporting impacts in the millions of dollars to recover.

In terms of today's ransomware attacks—that is why I say we were fortunate, because this was not a ransomware attack. In terms of today's ransomware attacks, you have to bring in cybersecurity experts, and, in some cases, rebuild many of your systems. It is absolutely just all-consuming, and cost range certainly in the several hundreds of thousands into the millions of dollars to do that quickly.

Senator HASSAN. Thank you.

Mr. Benitez, we started this conversation talking about the threat and then we talked about the impact on the local community. Before we start talking about specific solutions, I would like to hear from you about why it is important for victims to report incidents and how law enforcement and cybersecurity experts can help victims when they do.

Most people know of the Secret Service as the men and women in suits who protect the President of the United States, but the Secret Service also has an important role in combating cybercrime. How does the Secret Service help K–12 schools prepare for or respond to cyberattacks?

Mr. BENITEZ. Yes. Thank you for that question. To echo everybody's sentiments up here, first and foremost is working together in a preventative approach prior to an incident. Oftentimes, like you just spoke about, the budget constraints of an incident occurring, that money would be better spent, and school boards should realize that that money should be better spent on the front end for preventative measures. Prevention is definitely key for cybersecurity.

How the Secret Service—why it is extremely important to report is—it's important when we respond, when we receive a call from a victim, we will always respond to that victim in the State of New Hampshire. The reason being—to respond is we want to get in contact with the IT staff, maybe prior to the incident response team getting there, work with the incident response team, work with the insurance company, work with the third-party lawyer, to work with all those people that are involved so we can obtain those indicators

of compromise (IOCs), and tactics, techniques, and procedures (TTPs), so we can share that with the community.

It is important that we, in New Hampshire, do a better job moving forward that the public and the community understands reporting and getting everyone in this room involved early on and getting your local law enforcement, who have been through specialized training in NCFI, involved maybe even prior to an incident occurring so you are familiar with them, so intelligence that Rick does a great job sharing that comes from throughout the country could be shared to your information technology professional, if it is not in a formal document but—for example, when Nashua happened, I reached out to Wade Brown in Concord, and Wade reached out to Pam McLeod and said, "Hey, there is something happening." Luckily, she knew about it already. But these relationships are extremely important.

As a final thought of obtaining and providing these indicators of compromise to the community so there is not other victims, is there usually another victim. After Nashua hit, there was somebody in the Upper Valley that was hit a week later. It does happen in waves. Mostly there are some technical reasons. There is probably a recent exploit which has not been patched yet, which is understandable.

But, last, I wanted to mention is these crimes, everyone in the public, in the United States, need to realize these are usually transnational criminal organizations (TCOs) that are overseas that will be long-term investigations. You may not see a result tomorrow, but we have ascertained information in New Hampshire, provided it to task forces that are working globally to arrest suspects. We may not arrest somebody in New Hampshire, but we provide crucial data to further their investigation.

In addition, we are tracing and tracking cryptocurrency because it is available and open on the block chain to trace and track in perpetuity.

So it is important to cooperate and to coordinate, and do not be afraid to share this information. It is really a defense. It is really an individual defense and a national security defense to be cooperating with local, State, and Federal Government.

Senator HASSAN. Thank you very much both on the prosecution side of things, but on the prevention side of things for similar attacks to continue.

Is there a particular person a K–12 administrator should contact about a cyberattack?

Mr. BENITEZ. Yes. The easiest way, like I said, is contact the U.S. Secret Service at any time. We would like to meet you beforehand and work with Rick to go over your incident response plan. As we all have seen, personal relationships are a key to success. That is what we are about in New Hampshire. But also, to make it very simple, just search U.S. Secret Service in New Hampshire. There is a phone number, 24/7/365, you can get somebody live on the phone. We will respond.

Senator HASSAN. I take to heart the relationship-building part of it when you speak with task forces post terrorist events, for instance. We find that the most successful responses and the best way to prevent future attacks is when people have ongoing rela-

tionships and have worked together to prepare for the event, and that way, when the event happens, people are ready to go and they know what to do.

Go ahead.

Mr. KING. Madam Chair, I would like to add that in addition to the Secret Service's reporting capabilities, the Federal Bureau of Investigation (FBI) also runs IC3 and CISA has reporting capabilities. The important thing is is that any one of these resources that you contact, you are going to get us. We will collaborate effectively as to who is in the best location at the best time, place, and to be able to provide assistance as best we are able. It is very flat and it is very responsive.

Senator HASSAN. On that note, let me turn to the person whose job it is to make sure that these relationships continue and are flat.

Continuing this discussion of coordination and collaboration, Mr. Rossi, I want to again, say how grateful I am for your service and how pleased I am to welcome you to this panel as the first-ever cyber coordinator for New Hampshire.

You have been on the job now for 2 years. Could you tell us what you have been focusing on to help K–12 schools improve their cybersecurity?

Mr. ROSSI. Thank you, Madam Chair. The bulk of the work that I have been doing at this point is before an incident, working with IT directors to identify, manage, reduce cyber risk to their district. As most of the panelists have pointed out, every district is unique. Everybody has different problems. Everybody has different solutions. I have not been to a district that does not have a unique problem or a unique solution. That crosspollination of ideas is one thing, making those connections useful.

The primary area we are using right now is onsite cybersecurity assessments to identify vulnerabilities and provide mitigation guidance to districts before attacks happen. That looks at anything from preventing cyber-enabled fraud schemes, ransomware attacks, and cyber intrusions. We do a debriefing with the district, strongly recommending that senior leadership in the district is in the room to make sure that everybody has skin in the game. This is not a one-person IT director's problem. This is something we are making progress on over time. To conquer this is going to be a cybersecurity culture change.

We also connect them with no-cost technical resources, including CISA cyber hygiene vulnerability scanning, malicious domain blocking reporting for domain name system (DNS) filtering, as well as CISA's Secure Cloud Business Applications (SCuBA)gear, which is a more recent offering to assess optimal Microsoft 365 security configuration baselines, getting right to Pam's point that currently things are not secure by default. That is a major agency effort right now. Secure by design. Secure by default.

Everything is tailored. That is, anything from assistance to policy development, support to tailored assistance for each district, as well as technical assistance in looking at things like segmentation on a network.

Bottom line, ma'am, we take a look at where a district is, work with them where they are at instead of where they should be, and

help get them on a roadmap to progress them toward a more secure posture.

Senator HASSAN. Excellent. I know that you have met with a lot of school officials, but what message would you share with school officials who may not have had a chance yet to meet?

Mr. ROSSI. Appreciate the question, Madam Chair. The bottom line is CISA stands ready to partner with any of those districts. One of the common things that I keep hearing is "We are too small. It will never happen here." The message is the adversary gets a vote in that. While you may not think you are a great target, the adversary may think you are a fantastic target. Your ability to pay what you think is not a significant amount of money may be a significant amount of money to an overseas actor.

We are here to partner with you. One thing that I would point out is in one of my first school assessments, a superintendent said, "This is not what I was expecting at all. I was expecting multimillion-dollar projects that we do not have the budget for," whereas we are coming in and addressing some of the issues Pam just brought up, enabling security configuration within tools that are already paid for.

Ninety-five percent of cyberattacks involve human error. What we are trying to do is build a culture of cyber awareness leveraged onsite, and, again, that roadmap. We will start out with what is going to be lower costs, lower manpower hours, and start working our way up to things that are going to require greater financial investment.

Senator HASSAN. Great. Thank you so much for that.

Ms. MCLEOD. May I follow up on that really quick?

Senator HASSAN. Sure.

Ms. MCLEOD. Rick has been a fantastic resource for us. We need more of him. He is definitely overscheduled, scheduled far out. We definitely need more similar resources.

Senator HASSAN. OK. That is helpful. I will take that back to the appropriators.

Ms. MCLEOD. Thank you.

Senator HASSAN. Commissioner Goulet, with your help, 2 years ago, I spearheaded an effort to create a Federal grant program specifically targeted at improving the cybersecurity of State and local governments. This grant program was enacted as part of the bipartisan infrastructure law. Your work and support were critical in that effort.

I know that the Department of Homeland Security has only just begun awarding money under the program, but could you tell us how the grant program is helping K–12 schools improve their cybersecurity?

Mr. GOULET. Right off the bat, in advance of actually going through all the internal New Hampshire administrative hoops, we started moving on the multifactor authentication without actually having the money yet. One of the things I like to do is and one of the challenges with government in general is that there is a lot of administrative things that slow down progress, but sometimes you can legitimately get ahead of it.

While I am still waiting for the last couple of administrative steps so I can actually expend the money, we are actually out there

giving out these little keys that allow you to do multifactor authentication. I am like, "Why would you do a key? Because you could do it on your phone. You can do it through an authenticator application."

Pam brought up one of the reasons is that this idea from a union perspective that your personal device should not be used for work really does get in the way of that. We are addressing that very specifically with those keys.

But the other programs that we are implementing through the planning committee, .Gov in a Box, and the technical training are both shovel-ready, locked and loaded, and once we get through the last couple of steps—you know them well, Senator, in New Hampshire—then we will be actually ready to rock and roll on that.

Senator HASSAN. That is great. We have all spoken about it, but there are obviously a variety of State and local cybersecurity needs. How are K–12 schools involved in the process of applying for and awarding this Federal grant in New Hampshire?

Mr. GOULET. It starts with building community. The more effort we put into building community, the more people know what is going on and what opportunities exist out there. So that is where it starts. We will continue that forever.

Second, it is through the committee, the planning committee, and having representation on the committee that allows us to properly represent the needs of K–12s and the services we offer. That was, I think, a pretty huge deal.

We had a list of, I think, seven or eight projects. We put that before the committee, and they were like, "Oh, this is what we should do." It was a very collaborative process. Then making sure that we do not bundle. We have K–12s. We have municipalities. We have unincorporated places. Do not bundle them in a single thought pattern, but look at them individually. As Rick mentioned, you see some individual stuff everywhere. Again, I loved what you said about taking them from where they are and bringing them forward versus having this assumption of a certain level of competence.

Senator HASSAN. Got it. I have another question for you, Commissioner, and then I will follow up to Ms. McLeod.

In 2018, the New Hampshire legislature passed a law requiring the State Department of Education to establish minimum standards for the privacy and security of student data.

Commissioner Goulet, what, in your view, has been the impact of this law on K–12 cybersecurity in New Hampshire?

Mr. GOULET. I am going to tag-team. We are going to go "boom, boom" here.

Senator HASSAN. OK.

Mr. GOULET. But, initially, the impact was again, we had to look at it and say, "All right. What's happening out there?"

There was a lot of thrash going on. The main thing we did at first was how can we create a standard that was reasonable to implement?

There were a couple things on that. One was looking at Federal guidelines. Another was, taking an approach that was not too overly complicated and technical. The other was actually changing legislation, in other parts of State government, proposing changes so

that it potentially minimized the cost to K–12s in the sense that adherence to the standard was not layering cost.

I would ask Ken and Pam to talk about the downstream results of that.

Senator HASSAN. Yes, please.

Mr. WEEKS. If you do not mind, I think one of the big things that I came into this job looking at was risk that was being assumed by doing business with others. The CTO Alliance was ahead of that game. They had written up data standards, student privacy data standards, and insisted that vendors adhered to these and signed off on them before doing business with individual districts, et cetera.

My role in this was sort of acting as an advocate with other entities at the State level to ensure that the State did not undermine those efforts by having a standard that was significantly less, and potentially putting that same exact dataset at risk.

Senator HASSAN. Got it. Ms. McLeod.

Ms. MCLEOD. I will make one point first which is that New Hampshire's law also covers staff personal information. It is one of the few in the country that does. First we went into panic mode because this was massive for us.

Senator HASSAN. These new laws, requirements, right?

Ms. MCLEOD. Yes. In 2018. It was really overwhelming. We were not aware of it until almost after it passed. We did work with the legislators to kind of tone it down a little bit. Ken's predecessor, Dan Dister, and Ken, have just been a huge support for us in terms of developing those standards. They are based on network and information systems (NIS). They need to be revised at this point. It has been a few years. Really helping to understand how they apply to everything.

The grassroots effort was really because we had sort of no way to centralize this effort, so we, through the New Hampshire CTO council, which is our professional organization, and it's a State affiliate of CoSN, we developed a model which districts pay in just over a dollar per student per year, so it's a cost-sharing model. Very inexpensive, and it scales. We are all working together on these data privacy agreements. We have made huge progress. It has been really incredibly successful.

Senator HASSAN. Is it fair to say—I am looking at kind of how we talk about what K–12 schools in New Hampshire, what steps they have taken to date to implement this law. It is data privacy agreements. Anything else you would add to that?

Ms. MCLEOD. I would add that there is work from the Student Data Privacy Consortium, who we were a member of, on a national data privacy agreement that, from what I hear from the vendors, would be really significant for them. If we could get all of the States working together on one instrument that covered everybody? It is very difficult for the vendors to say, "Oh, we are going to meet this standard for New Hampshire, and this standard for California, and this standard for Texas."

That work is in progress, but if something could be developed maybe at the U.S. Department of Education, I think that that would really help vendors comply with the standards.

Senator HASSAN. Got it. Denis, you wanted to add?

Mr. GOULET. Just a quick follow-up, too. Like cybersecurity, privacy is a cultural thing. We need tools downstream, but if the culture is not supportive, it is hard to be successful. I think that cybersecurity culture evolution is a bit ahead of privacy cultural evolution in organizations, or at least in public sector organizations. I feel like building that culture is really important.

Business leaders, as was mentioned, you have to have your business leaders involved in cyber. Same thing with privacy. It is all of our responsibility to take care of that data.

Ms. MCLEOD. I could add, I found it, in Concord, very important to explain to our teachers, to put it in terms of what would happen if your child or your grandchild's identity was breached? They go to buy a car when they are 18, and somebody's purchased a house for them in some other State, under their identity.

Really putting it in those terms and helping them to understand how to freeze their credit, how to do those basic steps to protect accounts in their personal lives really helped reinforce with teachers that culture around privacy.

Senator HASSAN. That is great. Thank you.

Mr. Weeks, I want to turn to you because the Commissioner just told us that one of the ways the State and local cybersecurity grant program is helping New Hampshire communities is through the .Gov in a Box tool that you created. How does the .gov domain improve cybersecurity for local governments, including K–12 schools, and how did you come up with this idea?

Mr. WEEKS. First of all, I do not want to—it would be impossible for me to take sole credit for that. That was also a team sport. I will explain that a little bit.

But what .gov does is provides a verifiable identity for entities; whether that is a municipality, whether that is a K–12 district, it does not matter. It is verifiable. It is not easy to spoof. We have school districts and this is not pejorative, it is just the reality on the ground—that are .org, that are dot something, .US, I mean, you pick a domain, right?

Senator HASSAN. Right.

Mr. WEEKS. More and more, as some of these things age, they are easy to spoof. That can result in business email compromises. It can result in even more phishing attacks than if you are in a .gov domain.

The reason I say these other attacks is distributed denial of service (DDoS), et cetera—for example, if you go on NH.gov, we have that cloud hosted, and we apply DNS security to all of those domain names. That is a recent security improvement that we have implemented in the State.

Every K–12 that would sign up for .Gov in a Box—and I realize I might be getting ahead of myself a little bit here—would automatically have those protections as well. The identity verification, the nonspoofability, and the additional security that we will provide by our hosting mechanism are three great benefits for a K–12.

As far as .Gov in a Box, based on some data from the New Hampshire Municipal Association, only 26 percent of the eligible entities within the State of New Hampshire were on a .gov domain. The commissioner and I and a couple of other people looked at each

other, and we looked at the notice of funding opportunity (NOFO) and the priorities from CISA for the grant program, and one of the top ones was transition to .gov domains for those who are eligible.

We said, "Well, that is fine to tell them, but in New Hampshire we can not mandate them. We can just recommend this," as you very well know.

And so myself and Mr. Sgro kind of sat down and said, "What are all the reasons people would say no?" We started writing them down. We said, "Well, let us just add all that to the scope of services."

Regardless of where a K–12 or a municipality starts, at the end of the process, we will give you a turnkey solution to transition to .Gov in a Box, including your first box of stationery with your new website and email addresses on it.

Senator HASSAN. Got it. Yes.

Mr. WEEKS. Again, it was about what are all the reasons that someone may say no? Let us add that to the scope of services and concentrate on equity of outcome rather than an equal application of services.

Senator HASSAN. Got it. Thank you for that. Thank you to the whole team that has made .Gov in a Box possible. It is really exciting.

Mr. King, I want to turn back to you. Two years ago, I urged the Department of Homeland Security and Department of Education to improve their coordination efforts to protect K–12 schools from cyberattacks. The recommendation was to create a government-coordinating council which would work with Federal, State, and local governments to strengthen the cyberresilience of K–12 schools. I am pleased that the Department of Education recently announced it would be doing just that.

Can you explain, please, how the creation of this council will help Federal, State, local, and private sector entities coordinate their efforts to protect K–12 schools from cyberattacks? How is CISA working with the council?

Mr. KING. Thank you very much, Madam Chair. I think Pamela actually teed this up earlier. We are looking at how the Department of Education is trying to address these evolving lines, the dependencies within these technologies in order to still achieve their educational outcomes.

The important thing here is that—and Mr. Rossi mentioned this as well—that 95 percent of these risks are human related. Education is absolutely all about helping people understand how to best handle these challenges. It is an alignment that frankly, should have happened a lot sooner. But to bring both of these organizations together and then deliver that locally is absolutely critical.

You have seen what those here on the panel have said about Mr. Rossi. I see that consistently across the region, and my fellow chiefs across the country consistently see how important it is to have that trust and confidence in an individual or a group of individuals that are available and accountable for helping guide organizations along those paths to better security.

Senator HASSAN. Thank you.

Mr. Benitez, the National Computer Forensics Institute, which is operated by the Secret Service, offers training and equipment for State and local enforcement, for judges and prosecutors to combat cybercrime. You have mentioned it a couple of times. I am pleased to be part of that bipartisan group in Congress that pushed to reauthorize the Institute. I am glad it is reauthorized through 2028.

How has the National Computer Forensic Institute supported training investigations and other efforts here in New Hampshire?

Mr. BENITEZ. Yes. The NCFI—and kudos to the law enforcement professionals, judges, and prosecutors that have attended NCFI—they have really taken to understand cybersecurity, understand digital forensics. These are complex fields for law enforcement to get involved in and understand. But we have been able to use those resources. I think one of the overarching themes that is very positive to hear today is the NCFI, like the grant program, gives people like Pam actionable hands-on things to work on cybersecurity. We give the training. We provide the training free of charge. We provide the equipment, and it is brought back to the community to work on cybersecurity, the coordination with the other people throughout the country, the network of cybersecurity professionals to learn. Our law enforcement professionals will go down to Hoover, Alabama, and know that we have a group of people here—CISA, the State—and explain that to other law enforcement professionals in other States and develop those relationships throughout the country.

That is important, it is positive for New Hampshire and I am grateful that you are able to support that endeavor.

Senator HASSAN. Thank you very much. Again, trying to build awareness to what help is out there from a variety of different places and sectors to meet people where they are and help them get trained. It is really important.

Last question before the wrap-up question is to you, Ms. McLeod. As chair of the Alton school board, and as a former director of technology for a school district, you, I think—and you have demonstrated this—have a really unique insight into the budget resource challenges of K–12 cybersecurity.

In your view, what are the biggest challenges when considering resource allocation for K–12 cybersecurity and which budget items tend to be the most difficult to find funding for?

Ms. MCLEOD. I do not know if it is easily solvable, but I think staffing is the biggest issue. During the last year in Concord, I was spending about 75 percent of my time on cybersecurity and related sort of hardening cybersecurity and data privacy issues. That had increased gradually over the years.

There is also a massive infrastructure to run in Concord, so it is very difficult to give up the time. I think finding ways to supplement staffing or to free up staffing or bring in more staffing at sort of entry levels so it rolls up and the person doing cybersecurity has more time is the biggest issue.

Senator HASSAN. Great. Can you share with us some of the ways that New Hampshire schools have worked together to reduce the burden of expensive cybersecurity tools and services? You referenced some of them, but I think it is worth a little bit of focus.

Ms. MCLEOD. Yes. First of all, it is the collaboration. It is just massive. Some of my colleagues are in the audience. I have worked with many of these folks before that are up on the stage. But school districts where the IT folks are siloed, and do not collaborate, and do not sort of reach out, they are at most risk of cybersecurity issues. It is really important, I would say, for districts when they are selecting IT leaders to make sure that that person is collaborative and is going to reach out and work with others, because you can not do everything that you need to do.

Senator HASSAN. It is fair to say that when the spirit of collaboration is working among school districts and among various levels of government and various agencies, there are ways to share experience and share best practices that help each individual school—for instance, school district—lower its budget allocation for this, or at least try to save money and be as efficient as they can; is that fair?

Ms. MCLEOD. Absolutely. I think my colleagues are all really skilled at grabbing everything they can that's free, or grant funded. To give you an example, as I left Concord, I mentioned CISA's CrowdStrike offering. We did that through the little bit that was remaining out of our COVID ESSER funds. It is a pilot program, but we were able to put that into place. Actually, we put three or four layers of cybersecurity tools in place with those funds.

Everything you can grab from anybody just really makes up the difference, but it does take more time.

Senator HASSAN. Collaboration and coordination takes time.

Ms. MCLEOD. Yes.

Senator HASSAN. That is always one of the things we forget.

Mr. Weeks, did you want to say something?

Mr. WEEKS. One thing I will add is, I think, Senator, that all of the IT folks and the technical folks at the schools are very aware of the problem. One of the things is that we have tried to do—and it is a grant-funded training we have created cybersecurity training for both elected officials that school boards could take advantage of, as well as for more senior executives. Superintendents, principals could get this training. It is grant funded. Cost nothing to the municipality or the school district.

I think making those decisionmakers aware of these problems and the potential security weaknesses could influence budgetary decisions and administrative decisions going forward.

Senator HASSAN. And priorities, yes.

Ms. MCLEOD. Absolutely.

Senator HASSAN. All right. The wrap-up question here is to each and all of you. If you feel like you have already talked about it and, you do not have anything to add, that is fine, too, because I think this has been a really fulsome discussion and I am really grateful for it.

The final question to each of you is what more should Federal, State, and local leaders do to strengthen cybersecurity in schools? Anything else you would like to add?

We will go in this order. We will start with you, Mr. Benitez, and we will work this way.

Mr. BENITEZ. Thank you very much. Thank you for hosting this event today. I think, from a law enforcement perspective, we try to

stay on the preventative side, but we would really like to see, especially in New Hampshire, a grant-like program like the Internet Crimes Against Children (ICAC) has for cybersecurity in the public and private sector. What we are hearing here is it's hard to train and keep specialized people in information technology in the public sector and to keep law enforcement that has the skill set in law enforcement and not to go to the private sector.

I know in the Secret Service, for instance, we have a retention bonus. It would be nice to move some of these things that we learned in the Federal Government to the local government where we are providing money for people with specialized skills, increasing salaries where we can through bonuses.

Additionally, what many people do not realize, it is extremely expensive to purchase these software licenses. New Hampshire really needs to colocate our personnel. The Secret Service is working on this now. But, once again, it is difficult. There is not many personnel. People are strapped just for their normal duties rather than cybersecurity. But if we could coordinate from the public, Federal side, and the local law enforcement side together, colocated, saving money and spending on licenses at one location, I think that would be a tremendous asset for the citizens of New Hampshire to get more bang for their buck for response for cybersecurity.

One of the last things that we have done, we are in the midst of hiring someone who is not law enforcement but is a specialist in digital forensics, cryptocurrency tracing, and incident response, to work in our office as a Secret Service employee who would be there full-time, responsible to respond for the citizens of New Hampshire and work in a collaborative approach.

Thank you for your time today and hosting this event and very pertinent discussion.

Senator HASSAN. Thank you so much. Mr. Rossi.

Mr. ROSSI. Thank you, ma'am. Two things I would point out. We have already discussed resources. As the cybersecurity coordinator, I focus on K–12, but not just K–12. Even if I was just focused on K–12, you are talking a ratio of one cybersecurity coordinator to 90 school districts.

Additional resources. As we talked about the collaboration part, we all like each other, but we are almost forced to collaborate when there's one person here, one person there in the different agencies.

The last area I would hit on is having conversations like you have put together today here, Senator. Many school districts still view publicly disclosing a cyber incident as taboo, which, unfortunately, keeps the growing problem hidden. We are starting to talk about this in a national-level conversation. If someone broke into a classroom and stole all their computers, switches, and other technology, law enforcement would be notified, and that would likely be on the front page of the news. But when we have a cyberattack of the same magnitude, that is often swept under the rug and decisionmakers do not have the information on just how grave of a problem this is.

Again, Madam Chair, having conversations like this further the agenda. Thank you for having me today.

Senator HASSAN. Thank you very much. Mr. King.

Mr. KING. Thank you, Madam Chairwoman. Again, my compliments to bringing this forum together. I think it has been extraordinarily fruitful.

As you mentioned earlier, I previously worked in the commercial sector. When I worked with boards and senior executives, I would begin many of my conversations with "I want you to think about one aspect of your core business model that does not rely on information technology."

In the 3 years I have worked with that corporation, I never once got an answer. I occasionally got some functions that were not, but, bottom line was that very gradually, we have become completely dependent on these technologies.

We have to fix this. We have to get this right. We have to continue to try to reinforce this because the next wave is bringing even more complexity. If we can not get this right now, it is just going to get worse.

Senator HASSAN. I appreciate that very much. Thank you. Commissioner?

Mr. GOULET. A couple things. One is, with the advent of SLCGP, our traditional grant funding stream, which some years ago, the Homeland Security grants that are administered by the Department of Safety in New Hampshire and most other States, had a carve-out for cybersecurity.

There's now consideration in DC to kind of remove that because of the State and local cyber grant program which we have—we are not in favor of. I will say that very clearly.

I would like to work with you and anybody else on that and try to get visibility to it. We are also talking to the National Association of State Chief Information Officers (NASCIO) community as well to make sure there's visibility there.

The other thing is that part of the legislative intent is—for SLCGP, was get State and local governments used to investing in cybersecurity. I have spent some time in New Hampshire trying to do that. We have a State match in this biennium so that we can help our K–12s and municipalities. I want to keep that going.

From a local government perspective, I will be advocating for a continued investment. Because it harms us all it is not, "Oh, well, that school district got harmed." It is not a State issue. It really is. It harms us all when an individual entity is breached, when extra money is spent on what is essentially unproductive behavior, right? I will be advocating for that, and any support there is greatly appreciated.

Senator HASSAN. Thank you. Mr. Weeks.

Mr. WEEKS. Thank you, ma'am. We all, including all the K–12s across New Hampshire, have a significant amount of cybersecurity risk imposed on us by the fact that we have to do business with others. I won't beat around the bush. Specifically, the risk centers around software. The more that the Federal Government can help us by putting the pressure on vendors to be secure by design, secure by default. We, at the State level, do not have large enough voice to influence that conversation with the massive software vendors. Only the Federal Government can do that, in my opinion.

Helping us do that and not allowing them to continue putting security features behind paywalls that local governments, K–12s, and

State governments have a hard time affording and budgeting for would be a tremendous assistance.

The only analogy that I would use is if we bought a bunch of tanks and airplanes and artillery pieces that were as unsecured by design as the software had to be fixed, every taxpayer in the country would be up in arms over that.

Senator HASSAN. That's fair.

Mr. WEEKS. Thank you, ma'am.

Senator HASSAN. Thank you. Ms. McLeod, I wanted to give our representative of local government the last word here because this is really ultimately——

Ms. MCLEOD. No pressure.

Senator HASSAN. This is ultimately the level of which the impact of cyber breaches is felt the most directly. It really harms our kids and our schools and the staff and our taxpayers.

Ms. MCLEOD. Absolutely. To Daniel's point, IT touches every single aspect of a school district. There is not one part of a district that cannot be operated without technology. It is not just student personal information, but it is also behavior data, special education data, very sensitive data that we have seen breached in some of the big breaches like LA and in Minnesota. Stuff that people do not want to be splashed around the Internet.

One thing that districts can do is—that we have done in our district is put funds into a trust annually that's reactive, but to build something up to handle an emergency should it come up, whether it be infrastructure or cybersecurity. Federally, I think continuing the grants. I would love to see E-rate just focus much more on cybersecurity—actually, it does not build that focus on cybersecurity, cover MDR and SOC services, especially; cover other software pieces that can help secure the district; more Federal resources on the ground, like Rick; pushing the vendors to be secure by design. I think that's so important.

There is a paywall. Let districts pay for advanced features that they want, but not for cybersecurity. With both Google and Microsoft, you cannot even prevent an overseas login without going to features that are behind the paywall.

Other ed tech vendors have to pay attention to this as well, the smaller vendors.

Everything needs to be single sign-on or have multifactor authentication. That has to be built into every single tool that kids use. That is just really critically important to schools.

Senator HASSAN. I truly appreciate the discussion today. I thank you all for coming before the Subcommittee to discuss what is clearly a really important topic to a lot of us. I appreciate your hard work and your dedication to protect our communities, and specifically our kids from cyberattacks, especially right now as everybody's gearing up to return to school.

I think, the biggest takeaway I hope people watching today or listening to this or reading about it will take is that this is a responsibility that rests with each and every one of us, and we have to get more and more aware of the danger of cyberattacks. I think we have to invest time and resources and attention to prioritizing this, because the tools that we have in terms of education, in terms of what the digital world can provide educationally are really im-

portant and good, but we have to be able to engage in this space securely.

I thank you all very much, and I look forward to continuing to work with all of you. With that, this panel is adjourned.

[Whereupon, at 12:25 p.m., the roundtable was adjourned.]

○