AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. Hrg. 116–461

# STATE AND LOCAL CYBERSECURITY: DEFENDING OUR COMMUNITIES FROM CYBER THREATS AMID COVID–19

## HEARING

BEFORE THE

SUBCOMMITTEE ON FEDERAL SPENDING OVERSIGHT AND EMERGENCY MANAGEMENT

OF THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

ONE HUNDRED SIXTEENTH CONGRESS

SECOND SESSION

DECEMBER 2, 2020

Available via http://www.govinfo.gov

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

U.S. GOVERNMENT PUBLISHING OFFICE
43–278 PDF WASHINGTON : 2021

## COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

RON JOHNSON, Wisconsin, *Chairman*

ROB PORTMAN, Ohio
RAND PAUL, Kentucky
JAMES LANKFORD, Oklahoma
MITT ROMNEY, Utah
RICK SCOTT, Florida]
MICHAEL B. ENZI, Wyoming
JOSH HAWLEY, Missouri

GARY C. PETERS, Michigan
THOMAS R. CARPER, Delaware
MAGGIE HASSAN, New Hampshire
KAMALA D. HARRIS, California
KYRSTEN SINEMA, Arizona
JACKY ROSEN, Nevada

GABRIELLE D'ADAMO SINGER, *Staff Director*
DAVID M. WEINBERG, *Minority Staff Director*
LAURA W. KILBRIDE, *Chief Clerk*
THOMAS J. SPINO, *Hearing Clerk*

## SUBCOMMITTEE ON FEDERAL SPENDING OVERSIGHT AND EMERGENCY MANAGEMENT

RAND PAUL, Kentucky, *Chairman*

RICK SCOTT, Florida
MICHAEL B. ENZI, Wyoming
JOSH HAWLEY, Missouri

MAGGIE HASSAN, New Hampshire
KAMALA D. HARRIS, California
KRYSTEN SINEMA, Arizona

GREG MCNEILL, *Staff Director*
HARLAN GEER, *Minority Staff Director*
KATE KIELCESKI, *Chief Clerk*

# CONTENTS


| | Page |
|---|---|
| Opening statement: | |
| Senator Paul | 1 |
| Senator Hassan | 2 |
| Senator Rosen | 12 |
| Senator Sinema | 27 |
| Prepared statement: | |
| Senator Paul | 31 |
| Senator Hassan | 33 |


## WITNESSES

### WEDNESDAY, DECEMBER 2, 2020


| | |
|---|---|
| Brandon Wales, Acting Director, Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security | 3 |
| Denis Goulet, Commissioner, New Hampshire Department of Information Technology | 15 |
| John Riggi, Senior Advisor for Cybersecurity and Risk, American Hospital Association | 17 |
| Leslie Torres-Rodriguez, Ed.D., Superintendent of Schools, Hartford Public Schools | 19 |
| Bill Siegel, Chief Executive Officer and Co-Founder, Coveware, Inc. | 23 |


### ALPHABETICAL LIST OF WITNESSES


| | |
|---|---|
| Goulet, Denis.: | |
| Testimony | 15 |
| Prepared statement | 45 |
| Riggi, John: | |
| Testimony | 17 |
| Prepared statement | 51 |
| Siegel, Bill: | |
| Testimony | 23 |
| Prepared statement | 63 |
| Torres-Rodriguez, Leslie Ed.D.: | |
| Testimony | 19 |
| Prepared statement | 61 |
| Wales, Brandon: | |
| Testimony | 3 |
| Prepared statement | 35 |
| Responses to post-hearing questions for the Record: | |
| Mr. Wales | 81 |
| Mr. Goulet | 83 |

# STATE AND LOCAL CYBERSECURITY: DEFENDING OUR COMMUNITIES FROM CYBER THREATS AMID COVID–19

**WEDNESDAY, DECEMBER 2, 2020**

U.S. SENATE,
SUBCOMMITTEE ON FEDERAL SPENDING,
OVERSIGHT AND EMERGENCY MANAGEMENT,
OF THE COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS,
*Washington, DC.*

The Committee met, pursuant to notice, at 2:31 p.m. in room 342, Dirksen Senate Office Building, Hon. Rand Paul, Chairman of the Subcommittee, presiding.

Present: Senators Paul, Scott, Hawley, Hassan, Sinema, and Rosen.

## OPENING STATEMENT OF SENATOR PAUL[1]

Senator PAUL. I now call this hearing of the Senate Homeland Security and Governmental Affairs Subcommittee on Federal Spending Oversight and Emergency Management to order. The title of our discussion today is "State and Local Cybersecurity: Defending Our Communities from Cyber Threats Amid COVID–19."

In preparing for this hearing, it has become clear to me that good cybersecurity practices require a near constant struggle to stay ahead of events, and the real danger lies in getting complacent. Effective cybersecurity is an ongoing, everyday line of effort. The threat landscape is diverse, the best practices are constantly changing, the information you get may not always be reliable, the maintenance tasks can seem overwhelming, and most importantly, the stakes are high. In this context I have often found myself thinking, effective cybersecurity cannot move at, quote, "the speed of government."

By that I mean cybersecurity is a 21st century public policy problem, just is not solvable, or really even manageable by 20th century government means. Regulation, mandates, and centralized action, in general, these approaches are inadequate to match the pace of change that we have witnessed in the cybersecurity realm in recent years.

Congress needs to make sure that the government's role in detecting and responding to cyberattacks is clearly defined, and that they are focused, first and foremost, on the security of Federal information networks.

[1] The prepared statement of Senator Paul appears in the Appendix on page 31.

Today we will hear from the Department of Homeland Security (DHS) about their cybersecurity work—how it is evolving and their approach to this complex range of threats. With respect to individual actors in industries that are at the greatest risk of cyberattack—health care, education, financial services, retail, critical infrastructure—the proliferation of ransomware attacks over the past several months and years have made clear that these entities have to take on this responsibility themselves, on a day-to-day, minute-by-minute basis.

Irrespective of what the government is or is not doing, all cybersecurity is essentially local, and so today we will hear from experts in State government, the health care sector, and public education on their experience with cyber threats and incidents, and see the State of cybersecurity in these industries.

Fortunately for both government and the private sector, the marketplace for cybersecurity services is continuing to grow and mature. We will hear today from one such firm, Coveware, that consults with private and public entities on cybersecurity and works with them to respond to cyber incidents.

I would like to thank Ranking Member Hassan for suggesting this hearing, and I look forward to hearing from our panelists. Senator Hassan.

**OPENING STATEMENT OF SENATOR HASSAN[1]**

Senator HASSAN. Thank you very much, Mr. Chairman, for working with me to arrange this hearing and for your opening comments. I deeply appreciate the opportunity to continue working on an issue that I believe is critical to our national security, as well as to the economic security of our Nation.

State and local governments have been prime targets for cyberattacks for a number of years, but the stakes have only grown as coronavirus disease 2019 (COVID–19) has forced millions of Americans to migrate their everyday activities to the online world. Many students now learn from their teachers on a computer instead of in the classroom. Doctors treat many patients through telemedicine instead of in person. Governments handle many essential services online instead of at City Hall.

The massive increase in online activities over these past 9 months means that the targets for cyber criminals have increased commensurately. Unfortunately, cyber criminals have taken advantage.

One firm that tracks cyberattacks on schools and school districts reports that 44 attacks have occurred so far this school year and many more likely went unreported. We will hear from the superintendent of one of these schools today.

In the spring, Interpol warned that ransomware attacks against hospitals have grown significantly as hackers sensed an opportunity to extort more money in ransoms with hospitals overwhelmed with COVID patients. About a month ago, a cyberattack hit the University of Vermont Medical Center, forcing it to divert patients to other facilities, thereby jeopardizing the care of many

[1] The prepared statement of Senator Hassan appears in the Appendix on page 33.

patients, especially those in nearby rural areas who do not have the resources to travel to the next closest hospital for treatment.

The Federal Government has a responsibility to help protect our communities from these threats. While the Cybersecurity and Infrastructure Security Agency (CISA) has done a commendable job helping our State and local governments, the number and the severity of attacks on our communities continues to increase.

This hearing will help us identify ways for Congress and the Federal Government to better assist State and local governments in fending off these cyberattacks on our communities. We have a group of great witnesses who can help us work through these challenges, including CISA Acting Director Brandon Wales, who we are happy to have here today.

With that said, we are missing our original Federal witness, CISA Director Chris Krebs, because he was fired abruptly by the President 2 weeks ago. Director Krebs led CISA in a nonpartisan manner, and he approached his agency's most important task, securing the U.S. election infrastructure, with professionalism and tenacity. He was fired for doing his job, and we are less safe because of it.

It is imperative that we have strong, independent leadership at CISA going forward. As the Biden administration seeks to fill this position in 2021, I would encourage them to look to Director Krebs' example when considering his successor.

To all of our witnesses, I appreciate your willingness to testify, and I want to thank you all for the role you play in keeping us safe. I look forward to learning from your experiences as well as your expertise.

Thank you, Mr. Chairman, and I will proceed with introductions if you would like me to.

We will start, in this first panel, with our Federal witness. I am pleased today to introduce Brandon Wales, Acting Director for the Cybersecurity and Infrastructure Security Agency, at the United States Department of Homeland Security. Acting Director Wales was the first person to serve as the Executive Director of the agency before being very recently elevated to Acting Director. In this role, Acting Director Wales oversees CISA's efforts to defend civilian networks, manage systemic risk to national critical functions, and work with stakeholders to raise the security baseline of the nation's cyber and physical infrastructure.

Acting Director Wales, thank you for coming before the Subcommittee today, and I look forward to hearing your testimony.

## TESTIMONY OF BRANDON WALES,[1] ACTING DIRECTOR, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. WALES. Chairman Paul, Ranking Member Hassan, and Members of the Subcommittee, thank you for the opportunity to testify regarding the Cybersecurity and Infrastructure Security Agency's support to State, local, Tribal, and territorial stakeholders in mitigating a broad range of cyber threats facing our Nation.

[1] The prepared statement of Mr. Wales appears in the Appendix on page 35.

Whether focused on election security, responding to the digital transformation brought about by COVID–19, or addressing the plague of ransomware, I believe that enhancing and sustaining State and local cybersecurity capacity will be the defining cybersecurity challenge of the next decade.

This is my first appearance before the Committee in my new capacity as Acting Director, and I am honored to lead the men and women of our agency as we defend today and secure tomorrow.

I want to begin by thanking the CISA workforce and the entire election security community for their tireless work over the last 4 years, culminating in the November 3rd election. Our goal was simple: to make the 2020 election the most secure in modern history. We succeeded in building a robust election security community made up of State and local election officials, key Federal agencies, and private sector election vendors, in surging the technical capacity of CISA to improve cyber defenses nationwide and in harnessing the capabilities of CISA, the Federal Bureau of Investigation (FBI), the National Security Agency (NSA), U.S. intelligence community (IC), and the Department of Defense (DOD) to identify threats, respond to potential incidents, and take decisive action, when necessary.

As a result, layers of security and resilience measures are put in place by election officials and the community reacted quickly to disrupt efforts by foreign nations to interfere in the election. For example, we were able to rapidly share information on Russian intrusions into State and local networks, and attempts by Iranian government actors to send spoofed voter intimidation emails were publicly outed within 27 hours.

Our election security mission continues, and CISA will remain in an enhanced coordination posture until after election results have been certified in every State. We also stand ready to support States holding runoff elections in the coming months, such as Georgia and Louisiana.

This year has not only been focused on elections. Beginning in February, we have been working to support the nation's response to COVID–19, including helping to secure the development and distribution of potential vaccines under Operation Warp Speed (OWS). Since the pandemic's earliest days, we have seen malicious cyber actors targeting vaccine research and development, exploiting the dramatic expansion of remote work, and using COVID to advance criminal schemes.

In response, CISA ramped up information-sharing efforts on emerging threats, established a telework resource hub, and surged cybersecurity services to high-risk entities in the health care sector through our Project TAKEN. Now, under the Department of Health and Human Services (HHS) and DOD-led Operation Warp Speed, we are prioritizing services to companies deeper in the pharmaceutical supply chain to protect U.S. vaccine development and distribution.

Recently, hospitals across the country were hit with ransomware launched by a cybercriminal organization looking to profit from disruptions of critical health delivery during the pandemic. This was appalling, but not surprising, given the growth of ransomware incidents over the past 6 months. Ransomware is quickly becoming a

national emergency. We are doing what we can to raise awareness, share best practices, and assist victims, but improving defenses will only go so far. We must disrupt the ransomware business model and we must take the fight to the criminals.

While election security, a pandemic response, and ransomware may all look completely different, the one thing they have in common is a reliance on the networks at the State and local level. These are the networks that keep our communities running despite global challenges. These are the networks that help us respond to emergencies. These are the networks that run local hospitals and schools, and they are in need of urgent assistance.

CISA is taking action to help by strengthening operational partnerships, hiring additional cybersecurity coordinators to boost engagement in State capitals across the country, in supporting cyber proposals in the Federal Emergency Management Agency (FEMA) preparedness grantmaking process, and continuing to push CISA resources out from headquarters to where our partners are, in States and communities.

In conclusion, I want to thank the Committee for its leadership on legislation that has advanced the authorities of our agency and for your support for legislation still moving through Congress that will push CISA even further. This Committee has been an essential partner in our mission, and I look forward to continuing to work with you to defend today and secure tomorrow.

Thank you again for the opportunity to appear before you, and I look forward to your questions.

Senator PAUL. Thank you. Senator Hassan had to go vote so she will be back in a few minutes.

You mentioned, I believe, Russia and Iran, and it went by pretty quickly and I did not catch everything you had to say. You said these were attempts to actually change votes or to interfere in the election somehow? What did you exactly say?

Mr. WALES. Sure. The activity was a little different in both cases. In the case of Russia, Russia had launched a fairly broad campaign to target State, local, private sector, and Federal networks, using exposed vulnerabilities.

Senator PAUL. Using what?

Mr. WALES. Exposed vulnerabilities, fairly well-known vulnerabilities. They were looking for those vulnerabilities and trying to get inside of networks. We did discover that——

Senator PAUL. You are talking about election networks that count votes? What are you talking about?

Mr. WALES. I am talking about general networks. These could be private sector networks in things completely unrelated to elections. It did include, in one case, where they compromised a local county network and downloaded some information that had to do with the election. But this was not an attempt——

Senator PAUL. But this was not tabulation of the election.

Mr. WALES. No, absolutely no.

Senator PAUL. And what did you say about Iran?

Mr. WALES. Iran sent spoofed voter intimidation emails.

Senator PAUL. OK. Trying to disincentive people to vote, or something, to trick people into not voting.

Mr. WALES. Correct. They are trying to create a narrative that the election was——

Senator PAUL. But to your knowledge, there were no votes changed by a foreign actor. In fact, was that true? No votes were changed by a foreign actor, that you know of?

Mr. WALES. We have no evidence that votes were changed by an actor.

Senator PAUL. And no attempts were directly stopped. Is there sort of an existing voting network? You cannot really hack into a voting network, can you, that is just sort of there?

Mr. WALES. We have numerous advantages, in part because we have a highly decentralized system. There is not an election network. There are hundreds and thousands of election networks across the country. In addition, the actual vote tabulation systems, those are not networked on the Internet. The places where we see the most activity tends to be those highly centralized, internet-enabled systems, for example, voter registration or election night reporting. But even in those cases we did not see any adversary capable of compromising those systems to——

Senator PAUL. But it sounds like, as a general rule of thumb, if we are looking for advice on how to protect ourselves, the whole push of modern technology is to make us more connected, and maybe part of the advice is that we do not need to be too connected, having separate systems or separating. Is some of that advice taken within the Federal Government? You said we are protected in the electoral system because we have States and then we have counties and they are not completely integrated. We probably do not want to completely integrate or Federalize things with elections.

Is it true, within the Federal Government, that there is compartmentalization on purpose, to try to protect against hacking?

Mr. WALES. Yes. One of the major recommendations to any entity is to be thoughtful about how you network your systems, where you should segment your systems, where you should completely air-gap your systems. There is a reason why the classified networks that are operated by the intelligence community and Department of Defense are not accessible readily through the Internet. You want to keep those things separate.

Same thing for industrial control systems that operate the most sensitive, critical infrastructure in the country. You want to build additional barriers to prevent people from easily moving from small compromises onto parts of networks that could have much more significant consequences.

Senator PAUL. How much of the problem with attacking a network is coming through an email versus another way of attacking a network?

Mr. WALES. Frankly, it varies. Coming through an email, that normally includes things like spear phishing, where you get an email that says "click on this," and you click on a link and all of a sudden that malicious payload comes and compromises your computer.

I would say right now we are seeing, while that has been traditionally one of the more significant ways we have seen networks

compromised, over the last year we have seen dramatic growth in people compromising networks by exploiting vulnerabilities in virtual private network software. In part, this is as a result of the dramatic expansion of people teleworking, remote working, and a dramatic increase in the number of——

Senator PAUL. What does that mean? You are not attacking it through an email. You are attacking it through the cloud somehow, through software that communicates with the cloud?

Mr. WALES. Not necessarily the cloud but, for example, if you are connecting through a virtual private network, which is the way that maybe you call in to your company's network—I am at home, I am on my laptop, calling in to my company's network—I am connecting through a virtual private network (VPN) software. There are vulnerabilities in some of the more common VPN software, most of which have been patched, but if a company has not patched that vulnerability an actor may be able to exploit that vulnerability, compromise the connection——

Senator PAUL. But they are not logging into your computer. They are logging into your network and then bouncing back into your computer once again, if your network——

Mr. WALES. Or, more importantly, they want to get into that network, so they are exploiting that vulnerability to gain access to that network, and then once they are inside, using a variety of other vulnerabilities, they are trying to elevate their privileges. They have administrative capabilities, so they can create new accounts, and they can do whatever they want.

Senator PAUL. What is a guess on the percentage? How much of this is an email problem? Is half of it email, 75 percent, 25 percent? Just a guess.

Mr. WALES. It is a little bit hard to say right now. I would say probably at least half is still kind of spear phishing-related intrusions.

Senator PAUL. Right. Because it seems like that there would be a technological solution to some of that in really trying to protect email networks from the network, almost as if maybe you have a separate complete network that never communicates. They communicate with each other, so you can talk to each other, but never communicates with—I mean, almost somehow a complete separation of your email network from the rest of your network.

Mr. WALES. It is hard today, given the amount of interconnection between the various tools that you use in terms of any business. But most of the ways in which networks are compromised today are exploiting vulnerabilities where patches are available and where the solutions to mitigate these problems are readily available and they are just not being implemented by the information technology (IT) security professionals at companies.

Senator PAUL. How rapidly does it change? How rapidly does someone have to figure out that there is a brand new phishing or, technology?

Mr. WALES. You need to stay on top of it. Every day new patches are released for software. Now it may not be every single day for every piece of software, but on any given day there are new patches that come out for software. IT security professionals need to stay on top of that, understand what the nature of those vulnerabilities

are, and prioritize their efforts to close those vulnerabilities. Obviously, the bigger the network you have the more complicated this is.

Senator PAUL. When you come up with a patch, are you able to keep that somewhat secret from the criminals, or can they immediately see the patch and respond to the patch?

Mr. WALES. They can generally see it. These patches are made publicly available, so that as many individuals can protect their networks. It is a cat-and-mouse game. Every change we make on the defensive side, an offensive cyber actor is going to look to see what they need to do to get around that.

Senator PAUL. Are we able to, when we have a state actor that is going after classified information, and we have creative ways that State actors are using, are we able to share them with the private sector, or are we too worried that getting that knowledge out reveals that we know how to combat certain things? Are we sharing, on a consistent basis, knowledge that you gain with the private sector?

Mr. WALES. Absolutely. The partnership that we have with the intelligence community, in particular the National Security Agency, is better than any time in my entire 15-year history with the department. We are getting a significant amount of information from them, of things that they are seeing overseas, activity that they are seeing from foreign nations, getting that information to be declassified so that we can get it out to people, whether that is a specific incident at an individual location or, more importantly, information that could benefit the entire community.

A lot of the alerts that we are pushing out, alerting the community to different tactics that our adversary is using, are based upon intelligence sources that we are receiving from the intelligence community. That process is happening quickly.

Senator PAUL. Does it work both ways? Getting information back from private industry as well?

Mr. WALES. There is a vibrant cybersecurity community right now that has grown up over the past decade and a half, and there is a lot of information out there for everyone. We, ourselves, rely upon information provided by private sector cybersecurity firms to help improve our defenses at the dot-gov. There is a benefit to this community sharing as much information as possible, because that is the way we are going to have a more secure and a more defended cyber ecosystem.

Senator PAUL. As someone like myself who is very concerned with privacy, I have been concerned about having—I am all for telehealth and for allowing the Internet to allow us to see doctors remotely. As a physician, I think it is a good thing. But I am concerned about having a unique patient identifier where all of our data goes into one place and it is stored in one place. It goes back to this idea of compartmentalization.

When the Office of Personnel Management (OPM) was hacked, 22 million people's records were released, and I know that was a big mistake and hopefully we have learned from that. But there is a danger, and I think one way, from a patient point of view and from a point of view that there are sensitive things, whether you have an infectious disease that is acquired sexually, whether you

have a psychiatric disorder that you do not want the whole world to know about—there are a lot of things that could be very private.

Starting with my father 20 years ago and continuing today, we have been trying to get away from a unique patient identifier that the Federal Government has and I think it would be nice if people could equate that not only with privacy but also with the idea of hacking, that the more centralized your health care records are, it may be easier but it also might be easier for bad actors to get into your health community and extort people or damage them publicly with releasing private information. Any thoughts on health care security with regard to unique patient identifier?

Mr. WALES. I think that the challenges that you are describing there are the same challenges that we deal with in every cybersecurity challenge, and that is how do you balance the need to create more efficient, more effective systems with the risk that that poses because of the nature of connected systems being potentially vulnerable.

We encourage people to be thoughtful and take a really risk-based approach—how much information needs to be centralized, how much information needs to be networked—and be thoughtful. Then once you make that decision, then go to the next step and say, how do I defend the information that needs to be networked to the maximum extent possible? If I am going to have sensitive information that is Internet accessible, I need to make sure that my cybersecurity practices are going to be sufficient to defend that. I need to make sure that my patch management is good. I need to make sure that my configuration management is good.

Senator PAUL. Right, and I would just conclude by saying that the moral I get from your discussion on elections is there is some advantage to disconnectedness, to compartmentalization, to having counties, States, and the Federal Government be somewhat separate, where you can actually go to a county and verify an election. It does not go into some sort of mass network or computer. We are very lucky, I think, that we have sort of the Federal-State operation with regard to elections.

But I think people need to think that through before the efficiency experts say, oh, it would be so easy to have your medical records everywhere. They will be at every doctor, all of the time, anywhere in the United States, and they will be centralized. It is going to be easy until a hacker gets in there and all your private information is all over the Internet. I say be careful what you wish for, as some of those who really the centralization of things, because there is a danger of losing your privacy. Senator Hassan.

Senator HASSAN. Thank you very much, Mr. Chair, and I thank you for what you just covered in your questions. I want to start with a question really focusing on how we help State and local governments protect against cyber threats.

Acting Director Wales, your agency is responsible for securing Federal information technology infrastructure from a wide range of cyber threats. It is widely accepted that your work to secure the Federal space is critical. However, some might argue that it is not the Federal Government's job or responsibility to also try to secure State and local governments from cyber threats.

Let me ask you, does the Federal Government have an obligation or responsibility to also protect State and local governments from cyber threats?

Mr. WALES. Cybersecurity is a shared responsibility in multiple domains, and CISA takes seriously the responsibility we have to utilize the information, the knowledge, the expertise on cybersecurity to help all aspects of our critical infrastructure, whether those are State and local governments, if those are private companies operating our power grids, if those are hospitals or if those are chemical plants. We have a responsibility to help them.

Now, every system owner bears some responsibility for managing the security on their networks, and so I think it is trying to figure out where their responsibilities and our responsibilities intersect. We understand that we have a lot of information, we have a lot of expertise that we can provide. We can make sure that they are armed with all of the information that we have been able to glean from both the intelligence community, from our own visibility into the cyber activity of our adversaries, and the tactics that they are using, and it is our job to provide that as broadly as possible, to make sure that they are prepared.

Each of those individual asset owners needs to go through that process that Senator Paul and I just discussed, that risk-based process, to say how much security do I need in what parts of my network and how can I put that in place to be as robust as is required by the risks that I am facing?

Senator HASSAN. Thank you, and just to follow up, if a State or a community is vulnerable to cyber threats, how does that broadly impact the security of Americans who do not live directly in that State or community?

Mr. WALES. The State governments across the country, and local governments, operate some of our most critical infrastructure, whether it is operating water treatment facilities, in some States and communities, municipal power authorities in others. They also, obviously, at the State level, distribute significant amounts of funds through which Federal programs funnel money through.

States are a critical part of our fabric for both our economic and our homeland security. It is an important interest of the Federal Government that States have as much of our cybersecurity knowledge and expertise as possible to help safeguard those critical systems.

Senator HASSAN. Thank you. Various proposals have been introduced in Congress that establish a standalone Federal cybersecurity grant program for State and local governments that would pay for cybersecurity upgrades at the State and local level. Without specifically evaluating each bill, can you please describe for me the elements and considerations that Congress should be thinking about if we authorize a grant program of this nature? Are there any elements of a grant program that CISA views as being must-have items?

Mr. WALES. I think we would be happy to work with Congress on what a grant program would be, how a grant program could be structured to serve the maximum value. I would say until that time we have been working closely with FEMA over the past year as FEMA has required, as part of its last round of homeland secu-

rity grants, that a portion of it go to a certain set of high-priority items, including State cybersecurity. We spent the last year working with States, working with FEMA, to review the proposals that were submitted, and I think this will provide us a good baseline to understand how States are thinking about investing in cybersecurity utilizing Federal grants, how we can provide additional information to them to better shape and focus those grants on the highest-risk aspects of their networks.

But grantmaking is obviously a complicated topic, one that CISA does not have direct responsibility for managing, so I would probably refer you to people at FEMA who know more about kind of the grantmaking sausage. But at the more macro level, I think that we have a lot to add to help shape grants so that they actually target those things that we need to protect the most, and that it reflects the true partnership that exists between the Federal Government and our State and local governments on cybersecurity.

Senator HASSAN. Thank you. Cyber insurance is an important tool that helps companies and entities prepare for, prevent, and respond to cyberattacks. However, an August 2019 report by ProPublica revealed that if an entity has cybersecurity insurance, policyholders will use their cyber insurance policy to pay the ransom during a ransomware event, which, in turns, serves as a further incentive for hackers to launch ransomware attacks. The report also shows that hackers target cyber insurance policyholders because the likelihood of the victim paying the ransom is much higher.

During the COVID–19 pandemic, our country's increased dependency on online services may increase the incentive to pay ransoms so that critical services can be restored more quickly. Does CISA or your partner agencies generally know when an insurance company pays out a ransom?

Mr. WALES. As a general rule we have recommended against paying ransom, in part because it furthers the business model, as I indicated in my opening remarks. Ransomware is not going to go away as long as the business model is viable, as long as ransomware operators can do it.

Senator HASSAN. Right.

Mr. WALES. CISA generally focuses our efforts on ransomware before an event happens, helping companies prepare themselves, helping State and locals prepare themselves. We are generally not involved in decisions related to whether ransom is paid. That tends to be an individual decision at that company and they do not consult CISA as part of this.

Senator HASSAN. Generally speaking, you may not know if an insurance payment has been made.

Mr. WALES. That is correct.

Senator HASSAN. OK. Additionally, are cyber insurance companies working with you to tackle any of these negative incentives that seemingly drive more attacks?

Mr. WALES. I am not aware of engagement with cyber insurance companies on that issue right now.

Senator HASSAN. Do you think there is a role for Congress to play to help address this?

Mr. WALES. I think that this is an incredibly challenging problem. No one has cracked the code on what the answer is yet, and it is going to take more work between Congress and the executive branch to figure out what are the right tools we have to change the business model and to disrupt the business model on ransomware and make more progress in this space.

Senator HASSAN. Thank you, and, Mr. Chair, I see I am out of time. If we have a second round on this witness I will have one more question.

Senator PAUL. Senator Rosen.

**OPENING STATEMENT OF SENATOR ROSEN**

Senator ROSEN. Thank you, Chairman Paul, Ranking Member Hassan, for holding a hearing on protecting our communities from cyberattacks. During the COVID–19 pandemic the number of cyberattacks has significantly increased, and cyberattacks, of course, they are expensive, they are debilitating, especially for small organizations like schools, hospitals, and local governments. I am glad we are coming together in this bipartisan way to talk about how we can protect vulnerable communities, of course, in this challenging time.

But I want to focus on school cybersecurity because elementary schools, secondary schools, they face many challenges as they transition to online learning during the pandemic, including the constrained budgets, bridging the digital divide, ensuring the health and safety of students and faculty, and, of course, continuing to educate and support our students.

As schools struggle to meet these challenges they remain particularly vulnerable to hostile cyber actors. Earlier this spring, the FBI warned that K–12 institutions represent an opportunistic target to hackers. As many school districts, they just lack the budget and the expertise to dedicate to network integrity.

Last August, the Clark County School district, which is Nevada's largest school district and our country's fifth-largest school district, was the victim of ransomware attack. The hacker published documents online containing sensitive information, including social security numbers, student names, addresses, and grades. This is absolutely unacceptable and the Federal Government must find and help the schools obtain the tools and the resources to protect and combat these kinds of cyber threats, something I have raised with both CISA and the Department of Education.

Mr. Wales, can you speak to what steps CISA is taking to prevent cyberattacks, including these ransomware attacks like I had in Clark County School District, against K–12 schools, and how are you ensuring that we are not having more of these in the future?

Mr. WALES. Thank you, Senator, and I know that some members of the CISA team, along with the Department of Education, are planning on briefing you in your office later this week on this topic.

In the meantime, the first thing I would say is we have expanded our focus on K–12 education since the beginning of the pandemic, putting out additional information on how schools can improve their cybersecurity with their distance learning.

In addition, we are encouraging schools to participate through the information-sharing mechanisms that have been created, for

example, the Multi-State Information Sharing and Analysis Center (MS–ISAC), which is a free resource available, that we have invested in, from the Department, for State and local governments.

Today, 2,000 school districts, schools, and IT service organizations are part of that Multi-State ISAC, and there are additional resources and tools that States and school districts can take part in that can help them ensure their protection against ransomware and other attacks. For example, the MS–ISAC offers malicious domain blocking, so that known malicious domains that are used by ransomware operators would be blocked from activity on those networks.

But only about 120 schools are actively using that service that is offered for free today. What I want to see is much like we have done in the past 4 years in the election security context, how do we build a national community with the school districts to get them focused on the security aspects related to their networks that is not going to go away, even after the pandemic is over? We need to arm them with the same information, the same resources, and that is going to start with them taking advantage of the no-cost services that are currently offered across the country to State and local governments and the entities that exist within them.

This is obviously a big problem. There are over 13,000 school districts across this country. It is going to take time, attention, and focus. I am confident that if the Executive and Congress work together we can find creative ways of leveraging the capabilities that we have and getting more school districts signed up for these services.

Senator ROSEN. I appreciate that because I was going to ask you, I know you said 2,000 school districts are using it. In some cases now only hundreds of schools or school districts out of the 13,000. But you talk about malicious ware, ransomware. We have small school districts, rural school districts, that may not have the capacity or any expertise to even take advantage of your free services. Are there grant programs? What kind of support can we give, or that you can give, to be sure that the folks that are really sitting in those administrative offices can take advantage of what you are offering? Then we need to get it out there to 13,000 school districts, for sure, but not all of them have somebody who knows enough to really take advantage of it.

What are you doing there? What kind of programs are you offering for training for people who work in schools?

Mr. WALES. I think we have long recognized that the small and medium-sized businesses and government entities have unique challenges. What we had put in place earlier this year was something called CISA Cyber Essentials. These are the basic, bare minimum things that you need to put in place to get some baseline level of cybersecurity. It is geared for the small and medium-sized businesses and it is also geared for large companies to send out to their smaller suppliers to get them to a baseline level of security.

Over the past several months, we have been issuing monthly modules, toolkits, that could be used, step-by-step guides to take, for how to put in place the baseline level of cybersecurity. What are those things you need to do to make sure that you have challenging passwords, or two-factor authentication, how to set that up on your

network, making it a little bit clearer and easier for you to walk through.

But if States, if cities, if communities push that kind of information out, even to their smaller school districts, this is the kind of information that is powerful in the hands of those small companies, because the reality is ransomware operators are looking to make money quickly, and so they are going to look for whoever is the most vulnerable. If you have done some of the basics, if you have put in place the bare minimum level of cybersecurity, there is a good chance that that ransomware operator is going to go on to the next victim and they are not going to target you.

By investing a small amount of energy in putting in place cybersecurity, at even a bare level, you can have a significant impact and dividend for your overall level of security.

Senator ROSEN. I appreciate that, and my next question—I know I am out of time—would be we need the same kinds of things for our small businesses around the country as well. I look forward to speaking with you offline about how maybe we can get your message out for this training and the programs and all of the cyber hygiene to as many folks as possible, because we cannot afford not to communicate your hard work and what you have been doing to give people the ability to take advantage of these programs. Thank you.

Mr. WALES. Absolutely. I think any help we can get in amplifying the work that is already out there. The tools and resources that Congress has already invested in through CISA are available for all of the country to utilize, and we want more people to take up and use them. Anything you can do to get that message out there and amplify the work that we are doing, our agency is going to be grateful for.

Senator ROSEN. Wonderful. Thank you.

Senator PAUL. Thank you, Mr. Wales, and I hope you will be willing to respond to any questions we have in writing, if we have further questions from Members. I want to also thank you for reminding us that decentralization is a part of our defense against hacking of our elections, and as a great fan of the Federalist system that we had set up from the very beginning, even in our modern age, decentralization and compartmentalization are a big part of our defense and can make our elections more reliable.

Thank you very much for your testimony.

Mr. WALES. Thank you.

Senator HASSAN. I join the Chairman in thanking you for your testimony and for your service, and please, to all the women and men you work with, please take back our thanks as well.

Mr. WALES. I appreciate that and so do they. Thank you, ma'am.

[Pause.]

Senator PAUL. We are ready for our other panelists, whoever is in charge of that.

[Pause.]

We are doing the whole panel together, this panel, on one panel, if we can. Everybody can come in.

[Pause.]

OK. I misunderstood. These are virtual, so you can go ahead and do the introductions, Senator Hassan, please.

Senator HASSAN. Thank you very much, Mr. Chair. To all of our witnesses for this second panel, thank you for being here today, and I will introduce each witness directly before your testimony. I will start with our first witness, Denis Goulet.

I am pleased today to introduce Mr. Denis Goulet, who serves as Commissioner of the Department of Information Technology from my home State of New Hampshire. Commissioner Goulet has served admirably since he was appointed in February 2015. Commissioner Goulet also serves as President of the National Association of State Chief Information Officers (NASCIO).

Thanks for joining us, Commissioner Denis Goulet, and thank you for your exemplary leadership to strengthen cybersecurity efforts in New Hampshire and across the country. I look forward to your testimony.

**TESTIMONY OF DENIS GOULET,[1] COMMISSIONER, NEW HAMPSHIRE DEPARTMENT OF INFORMATION TECHNOLOGY**

Mr. GOULET. Good afternoon and thank you, Chairman Paul, Ranking Member Hassan, and distinguished Members of the Subcommittee for inviting me to speak today on the cybersecurity challenges facing State government that have been amplified during the COVID–19 pandemic. As Commissioner for the Department of Information Technology in New Hampshire and President of the National Association of State Chief Information Officers, I am grateful for the opportunity to highlight the vital role that State information technology agencies have played in providing critical citizen services and ensuring the continuity of government throughout this public health crisis.

Cybersecurity has remained the top priority for State CIOs for nearly a decade. There is growing recognition at all levels of government that cybersecurity is no longer an IT issue. It is a business risk that impacts the daily functioning of our society and economy, as well a potential threat to our nation's security.

State and local governments continue to be attractive targets for cyberattacks, as evidenced by the many high-profile and debilitating ransomware incidents. Inadequate resources for cybersecurity has been the most significant challenge facing State and local governments. The question of why Federal Government should be contributing to cybersecurity of the States is straightforward. States are the primary agents for the delivery of a vast array of Federal programs and services.

According to our recent national survey, State cybersecurity budgets are typically less than 3 percent of their overall IT budgets. Half of the States lack a dedicated cybersecurity budget. As State CIOs are tasked with additional responsibilities, including providing cybersecurity assistance to local governments, they are asked to do so with shortages in both funding and cyber talent.

Almost all the CIOs have the authority and are directly responsible for cybersecurity in their States, and have taken multiple initiatives to enhance the status of their cybersecurity programs. These initiatives include creation of cybersecurity strategic plan, adoption of the National Institute of Standards and Technology

[1] The prepared statement of Mr. Goulet appears in the Appendix on page 45.

(NIST) cybersecurity framework, development of a cyber disruption response plan, obtaining cyber insurance, and the implementation of security awareness training programs for employees and contractors. These initiatives are crucial as Congress considers the implementation of a cybersecurity grant program for State and local governments.

For the past decade, NASCIO has advocated for a whole-of-state approach to cybersecurity. We define this approach as collaboration among State and Federal agencies, local governments, the National Guard, education, K–12 and higher, critical infrastructure providers, and private sector entities. By approaching cybersecurity as a team sport, information is widely shared, and each stakeholder has a clearly defined role to play when an incident occurs.

My written testimony covers legislation that NASCIO has endorsed during the 116th Congress. I would like to reiterate my appreciation to this Subcommittee for its attention to cybersecurity issues impacting State and local governments. If passed, these bills would greatly improve our cybersecurity posture and create new, dedicated funding streams.

The pandemic has exacerbated the cybersecurity challenges for State IT. Since March, my colleagues and I have rapidly implemented technologies to allow State employees to telework safely and effectively in this new environment. We have helped our State agencies quickly deliver critical digital government services to citizens, including unemployment insurance. In New Hampshire, I have worked closely with our public health agencies to ensure they have the necessary tools to improve capabilities in the area of testing, contact tracing, case management, data analytics, and personal protective equipment (PPE) inventory. My colleagues and I have been honored to play a role in fighting COVID–19. We have taken on additional responsibilities and incurred new expenses while continuing to face unrelenting cyber threat environments.

I am truly concerned about how crucial IT and cybersecurity initiatives will remain funded in the coming months and years. States have seen significant declines in revenue and will be forced to make difficult budgetary decisions.

As President of NASCIO, I know I speak for all of my colleagues around the country when I say that a dedicated, federally funded cybersecurity grant program for State and local governments is overdue. Additionally, State governments should follow the lead of the Federal Government and begin providing consistent and dedicated funding for cybersecurity which will also require them to match a portion of Federal grant funds.

I look forward to continuing to work with the Members of this Subcommittee in creation of the grant program to improve our cybersecurity posture.

This concludes my formal testimony, and I am happy to answer your questions.

Senator HASSAN. Thank you, and I think we will move on to the next three witnesses, and then we will return for questions. Is Dr. Torres-Rodriguez available now? OK, she is back online.

Our next witness is Dr. Leslie Torres-Rodriguez, who joins us today from Connecticut. Dr. Torres-Rodriguez is the Superintendent of Hartford Public Schools, one of the largest urban

school districts in the State. Dr. Torres-Rodriguez was raised in Hartford and attended Hartford Public Schools. She has served as an education leader in the greater Hartford area for more than two decades.

In September, the Hartford School District was the victim of a cyberattack. Dr. Torres-Rodriguez, thank you for coming before the Committee today, and I look forward to your testimony.

Doctor, you might need to unmute yourself.

She is having connectivity issues, so why don't I do the other introductions and we will see if she is ready in a minute or two.

Our next witness will be John Riggi, Senior Advisor for Cybersecurity and Risk from the American Hospital Association (AHA). Mr. Riggi is the Senior Advisor for Cybersecurity and Risk for the AHA. He brings nearly 30 years of experience with the FBI, including serving as the Senior Executive for the FBI's Cyber Division Program developing mission-critical partnerships for the health care and other critical infrastructure sectors.

Mr. Riggi, I look forward to your testimony as well today, and I think we should probably proceed with that. Mr. Riggi, please feel free to proceed.

**TESTIMONY OF JOHN RIGGI,[1] SENIOR ADVISOR FOR CYBERSECURITY AND RISK, AMERICAN HOSPITAL ASSOCIATION**

Mr. RIGGI. Thank you, and good afternoon, Chairman Paul and Ranking Member Hassan, and Members of this Subcommittee. On behalf of our nearly 5,000 member hospitals and health systems the American Hospital Association thanks the Subcommittee for the opportunity to testify on this important issue, and we stand by, ready to assist as needed.

The AHA has a unique national perspective on cyber threats facing health care, stemming from our trusted relationships with the field and government agencies. The ongoing pandemic has resulted in a significantly increased cyber threat environment for health care providers. For example, this past October 28th, CISA, FBI, and HHS issued an urgent warning of an imminent ransomware threat to U.S. hospitals, and advised the field to take immediate defensive action. This threat remains ongoing as of today.

This threat also comes as hospitals and health systems were already dealing with what I call a COVID-induced cyber triple threat. The first threat is an expanded attack surface. In preparation and response to COVID–19, the health care sector rapidly deployed and expanded network-connected technologies such as telehealth, telemedicine, and telework. Unfortunately, this also greatly expanded network access points and opportunities for the cyber criminals to attack.

The second threat is increased cyberattacks. In conjunction with the expanded attack surface, cyber criminals have launched increased and relentless attacks on hospitals and health systems. HHS Office of Civil Rights (OCR) has reported a significant increase in hospital hacks since September 1, 2020, impacting millions of patients. Foreign intelligence services from China, Russia, and Iran, have launched cyber campaigns targeting health care, to

[1] The prepared statement of Mr. Riggi appears in the Appendix on page 51.

steal COVID–19 related data and vaccine research. Of all the attacks, ransomware attacks are a top concern. These attacks could disrupt patient care, deny access to critical electronic medical records and devices, resulting in canceled surgeries and the diversion of ambulances, thus putting patient lives and the community at risk.

The third threat hospitals face is resource constraints, due to reduced revenue as a result of canceled so-called elective surgeries and patients' reluctance to seek medical treatment during the pandemic. This situation leaves limited funds available to bolster network defenses and to recruit and retain scarce cybersecurity professionals. The above factors create a perfect storm of cyber threats for hospitals and health systems.

Regarding ransomware attacks, we believe a ransomware attack on a hospital crosses the line, from an economic crime to a threat-to-life crime, and therefore should be aggressively pursued as such by the government. Most often these attacks originate from foreign adversarial safe havens, beyond the reach of U.S. law enforcement. Combined use of military and intelligence capabilities, along with economic sanctions to augment law enforcement efforts, can reduce cyber threats to the Nation. By defending forward, the government can deter and disrupt these foreign-based cyber threats before they attack.

We believe a hospital victim of cyberattack is a victim of crime and should be provided assistance, not assigned blame. Despite regulatory compliance in implementing cyber best practices, hospitals and health systems will continue to be the targets of sophisticated attacks, which will inevitably succeed.

The government often repeats the phrase, "It is not a matter of if but when." Unfortunately, when a breach occurs, the Federal Government's approach toward the victims of cyberattacks is sometimes inconsistent across agencies and may be counterproductive. For example, Federal law enforcement agencies often request and need the cooperation of victims of breaches to further their investigations and disrupt the threat to the Nation.

Subsequently, or concurrently, a hospital or health system may become the subject of an adversarial investigation by the HHS Office of Civil Rights. This can be disruptive and confusing for the victim and stifle cooperation with Federal law enforcement.

Given the critical need to defend health care during the pandemic, along with the increased cyber threat environment, and a need to incentivize cooperation from victims, we strongly recommend that additional safe harbor protections from civil and regulatory liability be provided to hospital and health system victims of cyberattacks.

In conclusion, hospitals, health systems, and patients are heavily targeted by cyber criminals and sophisticated nation-states. Hospitals have made great strides to defend their networks, secure patient data, and most importantly, protect patients. However, we cannot do it alone. Health care needs more active support from the government, including consistent and automated threat information sharing, to help us defend patients and their data from cyber threats.

Conversely, the Federal Government cannot protect our nation from cyberattacks alone either. They need the expertise in exchange of cyber threat information from the field to effectively combat cyber threats. What is needed is an effective and efficient public-private cybersecurity partnership and a truly all-of-nation approach.

Thank you.

Senator HASSAN. Thank you so much. I want to turn now back to Dr. Torres-Rodriguez. If you are able to join us, Doctor, we look forward to your testimony.

**TESTIMONY OF LESLIE TORRES–RODRIGUEZ, Ed.D.,[1] SUPERINTENDENT OF SCHOOLS, HARTFORD PUBLIC SCHOOLS**

Ms. TORRES-RODRIGUEZ. Good afternoon, Chairman Paul, Senator Hassan, and Senators of the Committee. I am Dr. Leslie Torres-Rodriguez, Superintendent of Hartford Public Schools. We are the third-largest school district in Connecticut, with approximately 18,000 students.

I appreciate your invitation to address the Committee and answers questions regarding the cyberattack on Hartford Public Schools that occurred in September. The cyberattack had extremely disruptive effects on our school system, our students, and our staff. We were forced to postpone our first day of school, on September 8th, following months of intense planning for in-person learning amidst the COVID–19 pandemic.

While our students have been attending school, either in person or remotely, for nearly 3 months now, we are still repairing and recovering from lingering effects of the attack.

Hartford Public Schools and the city of Hartford were informed by our shared IT department, Metro Hartford Information Services (MHIS), that early in the morning hours on Saturday, September 5th, we experienced a severe cyberattack, specifically a ransomware attack which aims to take control of targeted servers and sell access back to the owner, back to us.

The attack was unsuccessful, overall, because Metro Hartford Information Services regained control of its servers without complying with the attacker's demands, thanks to recent cybersecurity investments and quick work by the Metro Hartford Information Services team.

Based on initial analysis by the Connecticut National Guard and the FBI, the attack was likely conducted by a highly sophisticated actor, and so in one sense we were fortunate that we avoided the worst case scenario.

Our district team, Metro Hartford Information Services, and Mayor Bronin's office worked late into the night on Labor Day, and in the early hours on Tuesday, September 8th, to ensure that Hartford Public Schools' critical systems were restored so that the first day of school could proceed.

Our student information system was restored around midnight, but as of 3 a.m. our transportation system was still not accessible. Our transportation company and our schools had no access to the student bus schedules. Around 4 a.m., I did have to make that dif-

[1] The prepared statement of Ms. Torres-Rodriguez appears in the Appendix on page 61.

ficult call to postpone the first day of school. Fortunately, we were able to get our transportation system back online the evening of September 8th, and we opened schools for the first time since March on Wednesday, September 9th.

However, 2 weeks later, our systems were still not yet fully operational and the costs to address the problem, financially and in terms of resources and staff time, have been significant. While we have regained control of servers and data, preventative measures are ongoing and present significant challenges to getting operations back to normal. For example, all of our servers needed to be taken offline and reimagined or restored from backups. The total amount of information that needed to be restored was over 70 terabytes across the city and school system, which is a massive amount of information.

Additionally, every computer that had connected to the district network before the attack, just before the start of the school year, had to be individually restored to factory settings before reconnecting with the network. This required a very fast deployment of new laptops to hundreds of staff members, which then depleted the stock of laptops that we had to provide to students at a very critical time in the school year. While we had ordered laptops with the intention of ensuring every student had a district device at the start of the school year, that plan was set back as a result of the cyberattack.

This was an especially difficult consequence of this attack as many of our students are participating in online learning from home and needed reliable devices to engage in their learning. These preventative measures impeded our ability to operate normally, and for our teachers to provide student instruction and impairing even basic functions like scanning and printing and having access to lesson plans.

I am proud of the work that has been done by our IT team, our city officials, and district administration, and thankful for the investigative actions and the support from the Connecticut National Guard and the FBI. However, we do need to protect our critical infrastructure by preventing such attacks in the future.

I thank you again, Senator Hassan, for inviting me to testify before this Subcommittee on this important issue. While the attack was unexpected and damaging in many ways, I am grateful for the way that our local, State, and Federal agencies collaborated to address the cyberattack and assisted with the restoration efforts. We are all committed to serving our constituents, our students, in the best way possible.

Thank you, and I will be happy to answer any questions that you may have.

Senator HASSAN. Thank you, Superintendent. I will now turn to the Chairman for an introduction.

Senator PAUL. Our final witness this afternoon is Bill Siegel, CEO and Co-Founder of Coveware. Mr. Siegel founded Coveware in 2018, to provide services to small and medium-sized businesses threatened by ransomware. They offer a full-spectrum suite of services, from identifying and closing vulnerabilities before an attack happens to decryption and navigation of an attack that has happened, to recovery after an attack.

Coveware and other private sector firms provide solutions that keep pace with the criminals. We are excited to hear from Mr. Siegel about the State of cybersecurity marketplace, what to do if your organization is attacked, and about low-cost steps that organizations of all sizes can take to enhance their cybersecurity posture.

Mr. Siegel, you are recognized.

Is he disconnected?

All right. Why do we not begin a round of questions with Senator Hassan, and we will get back to Mr. Siegel's testimony when he gets back on.

Senator HASSAN. Thank you, Mr. Chair, and I want to start with a question to Commissioner Goulet.

Commissioner Goulet, you and I know all too well the challenges of putting together a State budget. Giving more funding to the State's information technology budget might mean giving less funding to emergency services, education, public transportation, or other critical priorities. Moreover, when recessions happen, State revenues decrease, which leaves budget officials with even harder decisions to make.

Commissioner Goulet, can you talk about the challenges States face funding cybersecurity upgrades as they deal with reduced State revenues from the recent economic downturn? Do States have the ability to adequately fund their information technology budgets and better protect against cyber threats?

Mr. GOULET. Thank you for the question, Senator. We have some really recent data from the 2020 Deloitte NASCIO Cybersecurity Study, and I will share with you the top five barriers to overcoming cybersecurity challenges in State government: (1) lack of sufficient cybersecurity budget; (2) inadequate cybersecurity staffing, which really relates to number one; (3) legacy infrastructure and solutions to support emerging threats. The older systems tend to be much more vulnerable; (4) lack of dedicated cybersecurity budget; and finally, (5) inadequate availability of cybersecurity professionals.

I think that pretty well covers the gamut of the answer to that question.

Senator HASSAN. Thank you. I appreciate that. I will go on and complete this round.

Dr. Torres-Rodriguez, I want to turn to you, and I first just want to start by thanking you for participating in this hearing. All educators are facing unprecedented challenges right now, but to suffer a ransomware attack on top of everything else you are contending with means you are busier even than most other educators.

I want to start by getting a sense of where cybersecurity falls in the very long list of priorities that a school district like yours has. You mentioned in your testimony that there is a Metro Hartford Information Service. What sort of assistance do you get from them? Do you think that there are enough cybersecurity professionals to help the school district with the system you already have, and what sort of assistance from the Federal Government would be helpful, and did you receive before and after the attack?

Ms. TORRES-RODRIGUEZ. Yes, and just to give you a little more context, we have about 18,000 students and 3,400 staff members here in the public school system, and the shared IT department, which is managed by the city of Hartford, has six field IT techni-

cians in all. There is one staff member assigned full-time to cybersecurity, and that is across all of the city services. There is an opportunity, if you will, for additional support there.

With regard to the assistance from the Federal Government, Hartford Police and the FBI liaison there did investigate the attack and gather additional information. The Connecticut National Guard provided assistance with the recovery effort for about 4 weeks, primarily helping to mitigate and reimage our district devices. That was prioritized, and we are deeply grateful for that.

The National Guard has a team that specializes in defensive cyber operations, and their support was critical in assessing the attack and helping the Metro Hartford Information System team recover operations and help ensure security.

Overall, it was their assessment that this was a highly sophisticated and complex attack, that the information system team took a wide range of appropriate measures, but nonetheless it impacted school operations.

Senator HASSAN. Thank you for that. I am going to turn now to Mr. Riggi. Thank you for your work for our nation's hospitals, both in terms of your current position and from your time working for the FBI. As a cybersecurity professional who focuses on preventing cyberattacks to hospitals, can you please lay out for us the type of attack that most worries you?

Mr. RIGGI. Thank you, Senator. As I mentioned in my testimony, the attacks that I am most concerned about are ransomware attacks, which have the ability to disrupt patient care and risk patient safety. These types of attacks can lead to medical records becoming inaccessible at critical moments in treatment. Even understanding drug allergies for a patient may not be available. In certain instances we have had ambulances being diverted to emergency rooms which were further away from the original intended destination.

In the medical field, obviously, any delay in urgent treatment increases the risk of a negative outcome. Ransomware attacks, especially as we have seen the increase recently, is the top concern, certainly the most significant concern, that worries us at the moment.

Senator HASSAN. Thank you, and if I have a chance I am going to return to you with one more question. But first I do want to turn back to Commissioner Goulet.

Over the past decade, cyberattacks have increased in both their frequency and their ability to threaten our national security. Just as we have experienced with terrorism, the impacts of these cyber threats are not confined to far-off battlefield but to our States, our cities, and our communities.

However, as the threat has increased, Federal support for State and local governments has not increased commensurately. As you note in your testimony, only 4 percent of Homeland Security grant dollars have gone to support State and local cybersecurity over the past decade.

Can you provide your analysis for why you think that Federal funding for State and local cybersecurity efforts has not been commensurate with the threat? What do you recommend that Congress do in order to address this?

Mr. GOULET. Thank you. I so wanted to address that question in more detail. Myself and my colleagues around the country have really a queue of initiatives that we would do to help State and local governments, and education, and really all of the State, if we had access to more funds.

We have done as much as we could with those Federal Homeland Security grant funds that we were able to access, for example, in New Hampshire we built a nice Federal response program where we did take a whole-of-state approach. But we really could do so much more with dedicated cyber grant funding that flowed in in a separate stream. I think that although we are slowly improving our cyber posture in State we could very much accelerate the improvement of cyber posture with dedicated grant funding.

I would also like to reiterate that any such funding should include incentives for States to invest in a continuous manner as well.

Senator HASSAN. Thank you, and thank you, Mr. Chair.

Senator PAUL. Thanks. I do believe we see Mr. Siegel back online, and you missed your great introduction and you only get one introduction. But if you are there we would love to hear your testimony.

**TESTIMONY OF BILL SIEGEL,[1] CHIEF EXECUTIVE OFFICER AND CO-FOUNDER, COVEWARE, INC.**

Mr. SIEGEL. Thank you, Mr. Chairman, Ranking Member Hassan, and Members of the Subcommittee. Thank you for the opportunity to share Coveware's perspective regarding cybersecurity threats to State and local governments and small businesses. My testimony today is derived from Coveware's role in cybersecurity incidents from the perspective that handling thousands of these incidents has given us over the years.

Before we could try and solve this problem after we founded the company we recognized that something was missing. There was no clean data being collected on these incidents. The analogy that we used is you cannot build safe cars without visiting crash sites, measuring the skid marks and figuring out what happened.

Accordingly, when we founded the company we set out to build a large data set on what actually happens during these attacks. Our interactions put us right in the middle of these incidents. We work with forensic investigators, privacy attorneys, restoration firms, cyber insurance companies, and law enforcement branches of all kinds. The data that is exhausted and collected from these incidents, which span thousands of unique incidents, has given us a fresh perspective.

We use our data for three principal activities. First, we used it to contextualize these attacks for victims of these crimes, so they can understand how comparable companies have worked their way through these issues. Second, we aggregate these data findings and we try and publish our research, so to raise awareness of the very common attack methods that these actors use. Last, we provide a large subset of our data to law enforcement very readily to augment their active investigations.

[1] The prepared statement of Mr. Siegel appears in the Appendix on page 63.

A typical ransomware attack involves three phases. First is access. Almost all ransomware attacks are manually carried out. That means that the threat actor is physically inside the network of the victim, typically using stolen or harvested credentials.

The second is encryption, where the attacker employs an encryption program that locks up computer servers, and delete or encrypt backups as part of that process.

The third is extortion. This is where, if the company is not able to restore from backups, they are forced with a difficult decision of either having to pay a ransom or rebuild their network from scratch. While it may seem stark, this is a decision that hundreds of businesses face every single day.

Who are these criminals that carry out these attacks and what drives them? After thousands of cases and much study, we have a pretty clear picture of who carries out these attacks and why. By and large, the criminals that carry out ransomware attacks are financially motivated. Cyber extortion is their business, and the manner in which they conduct their business follows economic power laws. They seek profits just like legitimate businesses, and accordingly they follow strategies that maximize the outcome, minimize the costs, and increase the percent of their tax that they are able to monetize.

Why is cybercrime proliferating so rapidly? Following the economic theme, we estimate that a given ransomware attack can earn a single cybercriminal tens of thousands of dollars, with almost no risk, and profit margins well in excess of 90 percent. Economics 101 dictates that more activity will occur until the margins are driven down in this economy. It is simply too profitable and too low-risk to be ignored by would-be criminals.

Additionally, the cybercrime industry is innovated by an aim to attract new [inaudible] and thus lowering the barrier to entry for new criminals. We have detailed in our written testimony how Ransomware-as-a-Service allows a non-technical criminal the opportunity to participate. This combination of a highly profitable industry with low barriers to entry and a growing population of participants is the reason that these attacks are proliferating so much.

There are many ways to apply pressure to the economics of cybercrime. We offer one that we feel would be an effective means of curtailing activity. When we look at our own data, one sector stands out. Quarter after quarter, for the last 2½ years, a sector called Remote Desktop Protocol (RDP), is consistently the most used by ransomware actors. Properly securing our RDP is free. All it requires is a bit of time and effort.

As an example of how effective closing this vulnerability can be, I cite a recently published study that we cited in our written testimony, where a group of set out to proactively reduce the number of RDP-based ransomware attacks that occur. They contacted these companies, after proactively sustaining their networks, advised them of their vulnerability, and worked to patch this issue. The resulting 4 month period showed a 60 percent reduction in ransomware attacks across these organizations.

This is a free fix. All it takes is a little bit of elbow grease.

While this recommendation is just one example, we feel that there are further ways to attack the economics cybercrime, while

proactive security, new policy initiatives, and relentless pursuit of these criminals by law enforcement will never have substitutes in this fight. We think working big to small on reducing the profitability of cybercrime can produce immediate and material results.

Thank you to the Chairman, and I look forward to your questions.

Senator PAUL. Thank you for your testimony, and I am going to turn it over for further questions to Senator Hassan.

Senator HASSAN [presiding.] Thank you, Mr. Chair. I do want to return to our witnesses with some follow-up questions, and Dr. Torres-Rodriguez, I would like to start with you. You talked about the ransomware attack that the Hartford school system experienced. Now that it has been a few months since the cyberattack, can you please share with us what steps you have taken so far to try to prevent future attacks? What lessons have you learned?

Ms. TORRES-RODRIGUEZ. Yes. Prior to the attack, the city of Hartford had invested $500,000 upgrading the security system for Hartford Information Services, which is the shared services. That alone, helped us actually not have as significant of an impact as we would have had. Since then, new end-point security software called Carbon Black has also been implemented and installed in approximately 4,000 of our devices. What Carbon Black does is to leverage predictive security and is designed to detect malicious behavior and help prevent malicious files from attacking an organization, and can also assist with rapid restoration, which was one of our lessons learned, of critical infrastructure, should an attack happen again in the future.

Senator HASSAN. Thank you. I want to talk again to Mr. Riggi as well. You mentioned in your testimony some of the critical need for information sharing. Can you please lay out for us your assessment of cyber threat information sharing between the Federal Government and hospitals across the country, and between hospitals is it adequate or could more be done to improve cyber threat information sharing?

Mr. RIGGI. Yes. Thank you, Senator. I think I would characterize it as greatly improved compared to—one of the functions that I ran at the FBI was to disseminate information as we were just understanding how vital that information sharing is.

I think, one area that has been improved, has been the timely and actionable notices, highlighted October 28th notice I mentioned previously. For that information to be declassified and come out so quickly I think is very commendable, and to come out jointly by all three agencies is very commendable. However, I think there still needs to be more improvement in terms of regular cadence of sharing of cyber threat information, sharing it in a more automated and broad manner, and also the sharing of classified information, where possible, to trusted health care contacts.

It has improved but I think we still have a long way to go.

Senator HASSAN. Thank you. I understand that you work with hospitals across the country to help secure them from cyber threats. Can you give us the typical profile of a hospital cybersecurity staff, and how do small and rural hospitals differ in terms of cybersecurity professionals and resources as compared with major metropolitan hospitals, for example?

Mr. RIGGI. Yes, there is quite the range and spectrum of resources available, and the profile varies widely, generally, from small to large urban centers. Generally smaller hospitals have less resources in terms of less financial, human and technical resources to devote to cybersecurity. In many instances, these smaller, more financially challenged hospitals add on cybersecurity as a duty to, for instance, the chief information officer or IT director. Larger systems may have the luxury of having a very large staff. Multistate systems may have hundreds of people devoted to cybersecurity. However, they have vastly more complex systems and networks to protect and defend.

It varies widely. What I can say is that almost all hospitals now highly prioritize cyber risk as an enterprise risk issue, and are seeking to bolster their defenses. But they do struggle under the reduced revenue that they are facing as a result of COVID–19.

Senator HASSAN. Is that reduced revenue the major impact that you have seen with COVID–19 on this particular issue, or are there other ways that COVID–19 has affected, for instance, the staffing for hospital cybersecurity?

Mr. RIGGI. I think the reduced revenue has impacted staffing in the sense that certain hospitals may not have the financial resources to recruit and retain individuals. We have not seen a direct impact on COVID–19 reducing hospital cybersecurity staff, although there have been scattered reports of just general reduction in staff.

But ultimately I think that the staffing issue is a challenge for all sectors. Quite frankly, there is a zero unemployment rate for cybersecurity professionals, and hospitals are competing not only with other hospitals to recruit and retain but with other sectors and the government.

Senator HASSAN. OK. Thank you. I know that the health care sector has an Information Sharing or Analysis Center. Can you provide an assessment of how effective the health ISAC has been in assisting hospitals, and what are its limitations, particularly for small and rural hospitals?

Mr. RIGGI. The health ISAC, I think, has done a pretty good job of getting information out. I know the folks over there, good folks, and they do, as I said, a pretty good job. Some of the limitations may be in their reach, because they are a member-driven organization and they do require a membership fee. Now that fee is a sliding scale and may be fairly reasonable, depending on the size of the organization.

But again, I think that the issue there is the reach and timely dissemination. Often the H–ISAC relies on the government for the threat indicators as well. I think part of the mission of the H–ISAC and the government, going back to the CISA legislation of 2015, is to increase automated sharing of threat indicators, because the ability to share human to human, peer to peer, is just too slow to keep up with the adversaries. I think there still needs to be quite a bit of work done there, from both the government side and on the private sector side, to increase that electronic bridge for cyber threat information sharing.

Senator HASSAN. Thank you. I have a couple more questions but I understand that one of my colleagues, Senator Sinema, is online

and ready to ask her questions. Senator Sinema, I will recognize you for your round of questions.

**OPENING STATEMENT OF SENATOR SINEMA**

Senator SINEMA. Thank you so much, Senator Hassan, and I want to say thank you to our witnesses for participating today.

Even before this pandemic, cybersecurity was a critical issue in Arizona with ransomware attacks on Arizona medical, education, and government organizations. During the coronavirus pandemic, as more people go online for school, work, and social interactions, we have seen an increase in system vulnerabilities and cyber threats across the country and in Arizona.

Spending has also gone up as State, local, and Tribal governments work to support their community's information technology needs. As such, Federal cybersecurity support for State, local, and Tribal entities during this pandemic is critical.

Today I am going to direct my questions to Mr. Riggi. Medical devices with connectivity features are becoming more common in hospitals. In recent years, ransomware attacks on the medical community impacted not just hospital computers but also storage refrigerators. As coronavirus vaccines are approved, hospitals and health care systems across the country will be asked to accept shipments and store the vaccines under very precise conditions.

Has the American Hospital Association and its member hospitals created sound strategies to protect storage refrigerators and other systems that will be part of the vaccine storage and distribution plan?

Mr. RIGGI. Thank you, Senator. Our general guidance has been in terms of protecting all medical devices, to ensure that when they are, in fact, if they are, in fact, connected to networks that any potential vulnerabilities be identified and that they be network segmented. We will be closely monitoring the vaccine development and distribution, and we will certainly offer guidance to the field on how to protect those refrigerated devices. One of the main ways to protect them is to ensure that they are not network connected, and that if they are network connected to ensure that they are segmented and isolated from main networks and potential threats.

Senator SINEMA. Thank you. In 2019, as you may or may not be aware, Wickenburg Community Hospital, which is a hospital in rural Arizona, was hit by a ransomware attack. Wickenburg is a small, nonprofit hospital serving a community of about 8,000 residents. The hospital's four-person IT staff did not contact the cyber criminals to hear their demands. Instead, they began rebuilding the hospital's computer systems from scratch, using data the hospital had backed up onto physical tapes. The attack happened on a Friday, and by Monday the systems were almost fully functional again.

Now Wickenburg was unique for a small hospital in that it had an IT team with the expertise to rebuild the system. You mentioned constrained resources and shortage of qualified personnel as challenges to hiring qualified health IT security experts. What needs to be done to overcome these challenges, and how can Congress help?

Mr. RIGGI. Thank you. I think further incentives, perhaps, to recruit and retain cybersecurity professionals to work in health care, perhaps modeling other programs across government offering incentives for health care professionals, for doctors to work in rural areas, perhaps we need something similar to that for cybersecurity professionals.

As I said, unfortunately, there is a zero unemployment rate for cybersecurity professionals. Increased training, perhaps, of folks displaced from other services. Increased training, perhaps, or retraining of veterans as cybersecurity professionals may also be another plausible route to staff some of these positions.

Senator SINEMA. Thank you. The University of Arizona Medical School has studied the vulnerabilities of medical devices, and they have invited doctors, security experts, and government agencies to simulate a cyberattack on an infusion pump, a pacemaker, and an insulin pump, in 2017.

As you know, medical devices are regulated by the Food and Drug Administration (FDA) for both safety and effectiveness. What discussions have occurred between your hospital members, government regulators, and device manufacturers to prioritize the medical device security needs?

Mr. RIGGI. We feel we have been engaged quite a bit with the FDA concerning both their premarket and postmarket guidance on cybersecurity for medical device manufacturers. Although this still remains guidance, our position has been that we would like to see most of that, if not all of it, be made mandatory so that the manufacturers would have to comply with some of the guidance involving such concepts as security by design, making sure those features are built in, that the software bill of materials is provided by the manufacturer to the end user, so the end user can understand what the potential vulnerabilities may be in there, and also to provide lifetime support for the medical device, especially in terms of security upgrades.

We are constantly monitoring those issues. One of the things we advise our hospitals and health systems is to ensure that there is adequate communication between clinical engineering staff and the information security staff as well, to keep an accurate inventory of medical devices, identify vulnerabilities which may be present in those devices, and ensure that they are network segmented. Of course, the most precious lifesaving, life support devices like ventilators, are the ones that are most protected and segregated. Thank you.

Senator SINEMA. Thank you so much.

Madam Chair, I yield back the balance of my time, and I want to thank Mr. Riggi for taking the time to talk to me about these concerns in Arizona.

Mr. RIGGI. My pleasure. Thank you.

Senator HASSAN. Thank you very much, Senator Sinema. I have a couple more questions, and then assuming we do not have any other Senators join us we will adjourn.

I wanted to take the opportunity, Dr. Torres-Rodriguez, to turn back to you to get more of a sense from you about the impact that the recent ransomware attack has had on your community. As you discussed, it delayed the start of the school year, but can you share

with us how teachers, support staff, parents, and the rest of the community have been impacted by this cybersecurity attack, and how has the pandemic exacerbated these attacks?

Ms. TORRES-RODRIGUEZ. Yes. In terms of the ongoing operational effect of the attack, shutting down functions and servers did have debilitating consequences for a number of departments. For example, we did not have access to our financial management software for 17 days, so this caused delays in numerous financial processes, including our supply orders, year-end filing with our State requirements, grant filings, payroll, among other operations.

When I think about the broader implications, the disruptions to our school district, including that sudden delay to the first day of school after weeks of preparation, was disruptive to our families, given that already, as part of our mitigation efforts regarding our COVID mitigation, we did have a staggered, phased-in approach to return back to school. It caused disruption and confusion there.

The process of restoring well over 10,000 devices—laptops and desktops—for both students, teachers, and support staff, was tremendous. It did require a heavy lift in terms of human capital and time, which is, why the role of our IT department and the Connecticut National Guard, and even a third-party technical support that we have to contract out for, because otherwise we could not have done it. It would have taken additional weeks to start our school year.

During this time, our teachers did struggle to deliver quality instruction to both the 10,000 students that were learning online at home, as well as the 8,000 in their classrooms.

As part of the planning last spring and into the summer, we did make a decision to become a one-to-one district, meaning one device per each student, meaning that every student would have a district-issued device. There were over 2,000 devices that were no longer available for our students at the beginning of the school year because we had to prioritize getting our teachers to have their devices to deliver the instruction.

As I think about those early weeks, some of our students did not have access to learning, and we serve communities that have concentrated levels of need. Every minute, every day matters to us in terms of having access to instruction, and the other social and emotional supports that our students need to have.

Senator HASSAN. Thank you very much. That is very helpful.

Commissioner Goulet, I want to follow up on this issue of K–12 schools with you. Can you give us your thoughts, from the perspective of State governments, on how best to protect K–12 schools and hospitals? What role, if any, should State governments be playing?

Mr. GOULET. Thank you, Senator. This really is a great opportunity to highlight some examples of the whole-of-state approach that we advocate. I want to start by going back to a concept that Senator Rosen brought up earlier, which was this concept of making our activities consumable by those folks we want to help. If you have a small-staff school, you cannot throw sophisticated stuff at them, for them to absorb and have to do.

I know we have been working with MS–ISAC, on how we scale up some of their programs that were originally designed for State

governments but they need to be tweaked to be absorbed by schools in local government.

That is one area, but I think it is really being collaborative, involving these entities in planning. For example, in New Hampshire, on the school side, it is really being involved in the rollout of the minimum standards for security and privacy in schools, which was enacted by the State legislature in New Hampshire.

On the hospital side, we did involve local hospitals in our cyber disruption planning grant fund, the DHS grant funded cyber disruption planning. When we heard what was going up in Vermont, at the UVM Medical Center, we were able to reach out to cyber professionals and IT professionals in the hospitals in New Hampshire and find out what they were doing and whether they were preparing for or watching carefully to avoid this cyber risk of ransomware in the hospital, which, of course, as you have heard, is tremendous.

Those are some small examples there, and I think you really expect a collaborative, whole-of-state approach. What I use when I am speaking to people and trying to bring them into the tent, is there is no I in cyber.

Senator HASSAN. Thank you very much for that, Mr. Goulet, and thank you for your continued work for the people of New Hampshire.

I have a short closing statement and then I am going to go ahead, at the Chairman's request, and adjourn the hearing.

First of all, I want to thank Chairman Paul for working with me to organize this hearing, and I particularly want to thank his staff, Adam and Greg, for their work in making this happen. Again, I want to thank all of our witnesses for their testimony today, and for the role that you all play in helping to secure our nation from cyberattacks.

Cybersecurity at the State and local level has never been more important, and it is incumbent on all of us to work together to solve the unique challenges posed. It is clear to me that State and local governments, our K–12 schools, and our nation's hospitals all need additional resources and support to be able to achieve their missions in the face of cyberattacks.

I look forward to working with our witnesses and Members of the Committee on potential solutions, such as a standalone State and local cyber grant program, and improved information sharing between the Federal Government and schools and hospitals.

Thank you all for joining us today, our witnesses. I know how busy you are at this challenging time, and your contributions today make a world of difference, and we are very grateful.

Seeing that there are no other Members seeking recognition, I will thank our witnesses today again for their participation in this hearing. The Committee record will remain open until December 17th for Members to submit statements and questions for the record, and with that this Subcommittee stands adjourned. Thank you all very much.

[Whereupon, at 4:09 p.m., the Subcommittee was adjourned.]

# APPENDIX

---

Opening Statement of Chairman Rand Paul, M.D.
Subcommittee on Federal Spending Oversight & Emergency Management
*"State and Local Cybersecurity: Defending Our Communities from Cyber Threats amid COVID-19"*
*December 2, 2020*

I now call to order this hearing of the Senate Homeland Security and Governmental Affairs' Subcommittee on Federal Spending Oversight and Emergency Management.

The title of our discussion today is "State and Local Cybersecurity: Defending Our Communities from Cyber Threats amid COVID-19."

In preparing for this hearing, it's become clear to me that good cybersecurity practices require a near-constant struggle to stay ahead of events, and the real danger lies in getting complacent. Effective cybersecurity is an ongoing, everyday line of effort.

The threat landscape is diverse, the best practices are constantly changing, the information you get may not always be reliable, the maintenance tasks can seem overwhelming, and – most importantly – the stakes are high.

And in this context, I often found myself thinking: effective cybersecurity cannot move at quote "the speed of government."

By that I mean, cybersecurity as a 21st century public policy problem just is not "solvable" (or really even manageable) by 20th century government means. Regulation, mandates, and centralized action in general – these approaches are inadequate to match the pace of change that we have witnessed in the cybersecurity realm in recent years.

Congress needs to make sure that the government's role in detecting and responding to cyberattacks is clearly defined, and that they are focused first and foremost on the security of federal information networks. Today, we'll hear from the Department of Homeland Security about their cybersecurity work, how it is evolving, and about their approach to this complex range of threats.

With respect to individual actors in industries that are at the greatest risk of cyberattack—health care, education, financial services, retail, and critical infrastructure—the proliferation of

ransomware attacks over the past several months and years have made clear that these entities have to take on this responsibility themselves.

Irrespective of what the government is or is not doing, all cybersecurity is local, and so today we'll hear from experts in state government, the health care sector, and public education on their experiences with cyber incidents and the state of cybersecurity in these industries.

Fortunately, for both government and the private sector, the marketplace for cybersecurity services is continuing to grow and mature. We'll hear today from one such firm, Coveware Inc., that consults with private and public entities on cybersecurity and works with them to respond to cyber incidents.

I would like to thank Ranking Member Hassan for suggesting this hearing, and I look forward to hearing from our panelists.

Homeland Security and Governmental Affairs Committee
Federal Spending Oversight and Emergency Management Subcommittee

Ranking Member Margaret Wood Hassan
Opening Statement

Wednesday, December 2, 2020

Mr. Chairman, thank you for working with me to arrange this hearing. I deeply appreciate the opportunity to continue working on an issue that I believe is critical to our national security, as well as to the economic security of our nation. State and local governments have been prime targets for cyberattacks for a number of years. But the stakes have only grown as COVID-19 has forced millions of Americans to migrate their everyday activities to the online world. Many students now learn from their teachers on a computer instead of in the classroom. Doctors treat many patients through telemedicine instead of in-person. Governments handle many essential services online instead of at city hall. The massive increase in online activities over these past nine months means that the targets for cyber criminals have increased commensurately.

Unfortunately cyber criminals have taken advantage. One firm that tracks cyberattacks on schools and school districts reports that 44 attacks have occurred so far this school year, and many more likely went unreported. We will hear from the superintendent of one of those schools today. In the spring, INTERPOL warned that ransomware attacks against hospitals have grown significantly as hackers sensed an opportunity to extort more money in ransoms with hospitals overwhelmed with COVID patients.[1]

And about a month ago, a cyberattack hit the University of Vermont Medical Center, forcing it to divert patients to other facilities, thereby jeopardizing the care of many patients, especially those in nearby rural areas who do not have the resources to travel to the next closest hospital for treatment. The federal government has a responsibility to help protect our communities from these threats.

While the Cybersecurity and Infrastructure Security Agency has done a commendable job helping our state and local governments, the number and the severity of attacks on our communities continues to increase.

This hearing will help us identify ways for Congress and the federal government to better assist state and local governments in fending off these cyberattacks on our communities.

We have a great group of witnesses who can help us work through these challenges, including CISA Acting Director Brandon Wales, who we are happy to have here today.

[1] https://www.forbes.com/sites/daveywinder/2020/04/08/cyber-attacks-against-hospitals-fighting-covid-19-confirmed-interpol-issues-purple-alert/#4e597bc558bc

With that said, we are missing our original federal witness—CISA Director Chris Krebs—because he was fired abruptly by the President two weeks ago.

Director Krebs led CISA in a non-partisan manner, and he approached his agency's most important task—securing the U.S. election infrastructure—with professionalism and tenacity. He was fired for doing his job and we are less safe because of it. It is imperative that we have strong, independent leadership at CISA going forward.

As the Biden Administration seeks to fill this position in 2021, I would encourage them to look to Director Krebs's example when considering his successor.

To all of our witnesses, I appreciate your willingness to testify, and I want to thank you all for the role you play in helping to keep us safe. I look forward to learning from your experiences and your expertise.

Thank you Mr. Chairman.

**Testimony**

**Brandon Wales**
**Acting Director**
**Cybersecurity and Infrastructure Security Agency**
**U.S. Department of Homeland Security**

**FOR A HEARING ON**

**"*State and Local Cybersecurity:*
*Defending our communities from cyber threats amid COVID-19*"**

**BEFORE THE**
**UNITED STATES SENATE**

**Committee on Homeland Security and Governmental Affairs**
**Subcommittee on Federal Spending Oversight & Emergency Management**

**December 2, 2020**

**Washington, DC**

Chairman Paul, Ranking Member Hassan, and members of the Subcommittee, thank you for the opportunity to testify regarding the Cybersecurity and Infrastructure Security Agency's (CISA) mission to secure cyberspace and critical infrastructure. Our mission is to defend against the threats of today while working with partners across all levels of government and in the private sector to secure against the evolving risks of tomorrow – "Defend Today, Secure Tomorrow."

As the Nation's risk advisor, CISA leads the Nation's efforts to ensure the cybersecurity, physical security, and resilience of our critical infrastructure. CISA operates at the intersection of the Federal Government, state and local governments, the private sector, international partners, law enforcement, intelligence, and defense communities. By bringing together partners from across the critical infrastructure landscape, we enable the collective defense against cybersecurity risks, improve incident response capabilities, enhance information sharing of best practices and cyber threats, strengthen our resilience, and facilitate safety.

We share timely and actionable classified and unclassified information as well as provide training and technical assistance, and we do this in ways that prioritize the protection of privacy, civil liberties, and confidentiality. Specifically for State, Local, Tribal and Territorial (SLTT) Governments – which is the topic of today's hearing - the technical assistance and guidance provided can be used to secure networks, systems, assets, information, and data by reducing vulnerabilities, ensuring resilience to cyber incidents, and supporting their holistic risk management priorities. CISA's regional personnel are deployed in all States and territories to provide advisory services and assist the private sector and State and local government in improving their risk posture. With the support of this committee, CISA is in the process of hiring an advisor to serve in each State as a primary point of contact to improve State and local government cybersecurity.

As we continue to understand and support the management of the largest cyber threats facing our SLTT partners, a snapshot into what we have seen over the recent past could be grouped into three areas of focus: COVID-19 pandemic response and the mass shift to remote work and learning; cyber threats from ransomware; and election security. Independently, each of these threats is significant; taken together, they have the potential to stress systems and networks to the brink and we are working tirelessly to help SLTT leaders to defend today and secure tomorrow.

**COVID-19 Response**

Due to the global pandemic, the risk landscape shifted dramatically over the last eleven months. In March, CISA launched an effort to provide enhanced cybersecurity support to high-risk entities in the healthcare sector. When the Administration established Operation Warp Speed, CISA joined the interagency effort to offer cybersecurity services. In addition, CISA is leveraging its relationships with interagency and industry partners to facilitate greater communication and information sharing between the private sector, SLTT partners and the Federal government through coordinated alerts, guidance, and recurring engagement calls since the beginning of March.

CISA has been focused on understanding the impact of this shift and identifying organizations that are most critical to the response. Through our cybersecurity defensive services, our vulnerability scanning, and our information-sharing mechanisms, we are engaging with these critical organizations to assist them in establishing a strong defense today as well as a culture of resilience moving forward. In addition, we continue to assess the national critical functions, which allows us to identify and mitigate risk before it impacts critical infrastructure.

*Support to Operation Warp Speed*

Throughout Operation Warp Speed (OWS), CISA has focused on securing end-to-end COVID-19 vaccine production from research and development to manufacturing, and distribution, including countermeasures. Almost overnight, a set of American companies and institutions became indispensable, especially test labs, vaccine developers, and personal protective equipment manufacturers. CISA quickly began working with the Department of Health and Human Services (HHS), the Department of Defense (DoD), and the pharmaceutical industry to identify these entities and ensure they directly received necessary additional cybersecurity support, such as vulnerability scanning services, information sharing, and incident response.

CISA is working with its interagency partners on defensive activities, leveraging its relationships with government and industry partners to facilitate greater communication, coordination, prioritization and information-sharing between the private sector and the government through various alerts and guidance. We are also building cyber capacity by providing guidance for consumers and companies to increase cybersecurity maturity and awareness CISA's specific cyber defense/response activities include:

- Conducted 6 independent or joint notifications to OWS entities, covering open critical vulnerabilities, observed advanced persistent threat (APT) targeting or activity, or compromise.
- Provided 4 advanced warnings of state-sponsored cyber threats, which identified 2 additional entities targeted by APT 29 for information collection and 2 organizations potentially vulnerable to Chinese offensive activities.
- Provided notification of 8 critical vulnerabilities, helping to ensure that organizations patch appropriately to the risk level and where there may be increased risk of intrusion/affect from adversary cyber activities.
- Published 2 cyber advisory alerts highlighting APTs targeting OWS and 3 indicator bulletins.
- Conducted 6 incident investigations, including engagement with victims through initial forensics, malware and threat analysis.

CISA has also increased adoption of its Cyber Hygiene, which is a standard service offering that performs recurring scans of an organizations public facing IP addresses for known vulnerabilities with automated reporting to the organization, this service is available to all Federal agencies and designated critical infrastructure sectors. Cyber Hygiene services have increased from 5% of the

most important OWS entities to 62%, with 100% coverage of all OWS prime entities directly responsible for delivering vaccines.

CISA has also partnered with the Intelligence Community on the Overwatch service to better correlate existing intelligence collection to the infrastructure of key entities. This is a temporary intelligence and warning offering for OWS and related COVID response entities monitors threats involving the entities name, domains, and IP addresses. Overwatch adoption has gone from 0% to 62% with 100% coverage of the primes. CISA has also pledged to deliver monitoring services to up to 15 companies, with multiple companies currently going through the adoption and onboarding process and 17 separate detailed cyber vulnerability and architecture assessments and 10 field-based physical security assessments.

*Essential Critical Infrastructure Workforce Guidance*

Beginning in March, CISA released the Essential Critical Infrastructure Workers Guidance (ECIW), providing assistance and guidance to States and jurisdictions as they considered how to prioritize and support essential workers to operate safely while supporting ongoing infrastructure operations across the Nation. The guidance is advisory and seeks to identify, through analysis and coordination with Government Coordinating Councils and Sector Coordinating Councils, those critical infrastructure sectors, workers, and functions that should continue to work safely during the COVID-19 response across all jurisdictions. Through several updates issued throughout the Spring and Summer, CISA was able to account for the changing landscape of the Nation's COVID-19 response to support SLTT decision makers.

Early versions of the guidance were primarily intended to help officials and organizations identify essential work functions in order to allow them access to their workplaces during times of community restrictions. CISA's final release, Version 4.0, highlighted additional essential workers and specialized risk management strategies to ensure that personnel can work safely as States re-open. CISA will continue to work with our partners in the critical infrastructure community to update this advisory list if necessary, as the Nation's response to COVID-19 evolves.

*CISA COVID – 19 Resources and Alerts*

In addition, CISA is providing a one-stop-shop of cybersecurity and critical infrastructure resources from across Federal, private sector, and international partners to raise their security posture in this new landscape. Some of these resources include:

- *Cyber Essentials Toolkit*: A set of modules designed to break down the CISA Cyber Essentials into actions for IT and C-suite leadership to work toward full implementation of each Cyber Essential element.
- *CISA Trusted Internet Connections 3.0 Interim Telework Guidance*: Focuses on remote Federal employees connecting to private agency networks and cloud environments in a secure manner.

- *Best Practices for Industrial Control Systems*: Released with the Department of Energy, and the UK's National Cyber Security Centre (NCSC).
- *COVID-19 Recovery CISA Tabletop Exercise Package*: Developed to assist private sector stakeholders and critical infrastructure owners and operators in assessing short-term, intermediate, and long-term recovery and business continuity plans related to COVID-19.
- *Critical Infrastructure Operations Centers and Control Rooms Guide for Pandemic Response*: The guide provides considerations and mitigation measures for operation centers and control rooms but can be applied further to any critical node that is required to continue functioning in a pandemic environment.
- *CISA Insights: Risk Management for Novel Coronavirus (COVID-19)*: Provides executives a tool to help them think through physical, supply chain, and cybersecurity issues that may arise from the spread of Novel Coronavirus, or COVID-19.
- *Security and Resiliency Guide – Healthcare and Public Health Facility Annex:* This resource provides information to assist stakeholders with performing counter-improvised explosive device activities specifically applicable to healthcare and public health facilities.
- *Physical Security Considerations for the Healthcare Industry During COVID-19 Response:* Is a jointly developed product among CISA, Health and Human Services (HHS), and Federal Bureau of Investigation (FBI). It provides information regarding potential physical threats posed to the healthcare community during the pandemic.

Since the outbreak of COVID-19 in March 2020, and in collaboration with domestic and foreign partners, CISA provides up-to-date cyber threats and COVID-19 alerts. Some of our more recent alerts include:

- *Ransomware Activity Targeting the Healthcare and Public Health Sectors:* This joint cybersecurity advisory was coauthored by the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the Department of Health and Human Services (HHS). This advisory describes the tactics, techniques, and procedures (TTPs) used by cybercriminals against targets in the Healthcare and Public Health (HPH) Sector to infect systems with ransomware.
- *Chinese Targeting of COVID-19 Research Organizations*: CISA and FBI Joint Alert warning that the People's Republic of China (PRC) is likely targeting organizations researching COVID-19.
- *Cyber Warning for Key Healthcare Organizations in the UK and USA*: The UK's National Cyber Security Centre and CISA have exposed malicious cyber campaigns targeting organizations involved in the coronavirus response.
- *COVID-19 Exploited by Malicious Cyber Actors, Joint UK, and US Alert*: This alert provides information on exploitation by cybercriminals and advanced persistent threat (APT) groups of the current coronavirus disease 2019 (COVID-19) global pandemic.
- *Enterprise VPN Security Alert*: Alert encouraging organizations to adopt a heightened state of cybersecurity when considering alternate workplace options for their employees.

To address the increased risk introduced by expanded telework during the COVID-19 pandemic, CISA has built an online portal for telework, addressing an array of issues, including remote patching, securing sensitive and proprietary data, and incorporating virtual collaboration tools. The Telework Center of Excellence portal brings together in one place products from

across the Federal government and private sector, including CISA, the Office of Personnel Management (OPM), National Institute of Standards and Technology (NIST), Cyber Readiness Institute, National Cyber Security Alliance, and the Global Cyber Alliance. Key recent releases include:

- *Cybersecurity Recommendations for K-12 Schools Using Video Conferencing Tools and Online Platforms*: A video conferencing product for a school district and campus IT administrators and staff charged with securing their IT networks, as well as end-users, such as teachers, to help them think through their cybersecurity issues.
- *Video Conferencing: Guidelines to Keep You and Your Students Safe*: A one-page tip sheet for schools using video conferencing.
- *Guidance for Securing Video Conferencing*: A product for organizations and individual users leveraging video conferencing tools, some of whom are remotely working for the first time.
- *Cybersecurity Recommendations for Federal Agencies Using Video Conferencing*: A product for executives charged with securing Federal agency networks, and for Federal employees to help them think through related cybersecurity and physical issues.
- *Cybersecurity Recommendations for Critical Infrastructure Using Video Conferencing*: A product for executives charged with securing critical infrastructure networks and for critical infrastructure employees to help them think through related cybersecurity and physical issues.
- *Telework Best Practices with CISA and NSA*: A joint-seal product from CISA and NSA featuring "Do's" and "Don'ts" for teleworking.
- *Tips for Video Conferencing*: A tip sheet with top recommendations on how to safely videoconference, with tips such as: 1) Only Use Approved Tools; 2) Secure Your Meeting; 3) Secure Your Information; and 4) Secure Yourself.

Additional resources and alerts can be found at https://www.cisa.gov/coronavirus.

*COVID-19 Emergency Communications – Assistance and Alerts*

Throughout the COVID-19 response, our Nation's public safety communications across the Federal and SLTT landscape have been tested as never before with the nationwide shift to a virtual environment. Emergency communications need to work the first time, every time, during all threats and hazards that threaten lives and property.

A decade of emergency communications interoperability preparations and planning was critical in mitigating impacts of COVID-19 and the stress placed on emergency communications. CISA's work with long-standing partners, including SAFECOM, the National Council of Statewide Interoperable Coordinators (NCSWIC), and Federal department and agencies, provided a clear understanding of emerging requirements and the ability to act decisively. Together with the Statewide Interoperability Coordinators (SWICs), CISA was able to operationalize the National Emergency Communications Plan to support an evolving ecosystem and those on the front line; increase connectivity to priority networks for essential workers to

mitigate network contestation, seeing a dramatic increase of Priority Telecommunication Services (PTS) use, expedited over 70,000 PTS activations, and support to several major hospitals, medical centers, and critical infrastructure manufacturers; and, developed critical emergency communications policies, guides, advisories, and technical standards, including:

- *Guidelines for Executives: 911 Center Pandemic Recommendations:* Emphasizes the importance of communication centers, accentuates the particular risk of a pandemic to resiliency of 911 operations, communicates executive-level action, and describes available guidance for 911 administrators.
- *Guidelines for 911 Centers: Pandemic Planning:* Highlights governance, resource planning, and contingency considerations from a holistic perspective during a pandemic.
- *Guidelines for 911 Centers: Pandemic Operating Procedures:* Recommends how to organize, train, and care for personnel while operating during a pandemic.
- *Guidelines for 911 Centers: Cleaning and Disinfecting During a Pandemic:* Presents cleaning and disinfecting guidance specific to public safety and resources for 911 centers during a pandemic.

**Ransomware**

Cybersecurity threats are all around us, and ransomware is a specific malicious type of cyber threat that has been in the news a great deal lately. Ransomware is a type of malicious software, or malware, designed to deny access to a computer system or data until a ransom is paid. Ransomware can be devastating to an individual or an organization in the form of disrupting critical public safety services, placing personal information at risk, and potentially losing millions of dollars financially. Ransomware continues to be a significant threat facing U.S. critical infrastructure, SLTT, and the private sector.

Ransomware has rapidly emerged as the most visible cybersecurity risk playing out across our Nation's networks. In just the past few months, several hospital systems across the country and the globe were affected by ransomware. In October, the University of Vermont Health Network was reported to the targeted of a ransomware attack that impacted a variety of patient services, including access to medical records. The network has restored access to electronic medical records, but is still in the process of restoring all its services.[1]

Additionally, multiple hospital systems and healthcare providers across the U.S. have incurred ransomware attacks creating varying degrees of impact. In October, CISA, in coordination with the FBI and HHS issued a joint cybersecurity advisory warning the Healthcare and Public Health (HPH) Sector of increased and imminent threats to healthcare providers from ransomware attacks.[2]

---

[1] "University of Vermont Medical Center Continuing Cyber Attack Recovery." Insurance Journal. December 1st, 2020. Accessed here.

[2] Alert AA20-302A, Ransomware Activity Targeting the Healthcare and Public Health Sector, Cybersecurity and Infrastructure Security. October 28, 2020. Accessed here.

CISA has several tools, products, and services to help protect against cybersecurity risks and vulnerabilities, like ransomware, including:

- *Joint CISA/ MS – ISAC Ransomware Guide:* A one-stop product for Ransomware Prevention Best Practices and includes a Ransomware Response Checklist, information on available risk management services from CISA, and explains how to request analysis and response assistance from the Federal Government.
- *CISA Insights: Ransomware Outbreak:* Provides stakeholders an understanding of how ransomware attacks unfold and what steps organizations can take to better defend their systems.
- *Protecting your Center from Ransomware:* Provides comprehensive information to stakeholders on how to protect public safety answering points (PSAPs) and emergency communications centers (ECCs) from ransomware.
- *Cyber Risks to Next Generation (NG911) white paper*: Provides an overview of the cyber risks that will be faced by NG911 systems.
- *NG911 Readiness Self-Assessment Tool*: The NG911 Self-Assessment Tool helps ECC/PSAP administrators and oversight personnel evaluate a system's NG911 maturity state and understand the next steps necessary to continue NG911 deployment progress.
- *Cyber Risks to 911: Telephony Denial of Service Fact Sheet:* This fact sheet familiarizes public safety communications partners with Telephony Denial of Service (TDoS) threats to 911.
- *Cyber Assessments:* Based on NIST 800-53 framework; reviews processes and procedures and areas of improvement.
- *Ransomware Awareness/Education Brief for PSAP, 911 and LMR Operations*: Provides best practices for secure use of technologies in daily operations, including interactive webinar with PSAP/9-1-1/LMR operations staff.

**Election Security**

CISA leads DHS efforts to secure our nation's election infrastructure. CISA, our Federal partners, state and local election officials, and the private sector prepared for the 2020 elections for nearly four years. Due to the exceptional efforts of the election community, at this time there is no evidence that any voting system deleted or lost votes, changed votes, or was in any way compromised. Since 2016, CISA has led a voluntary partnership of Federal Government and election officials who regularly share cybersecurity risk information. CISA has engaged directly with election officials—coordinating requests for assistance, risk mitigation, information sharing, and incident response. To ensure a coordinated approach to assisting election officials with protecting the election infrastructure they manage, CISA has convened stakeholders from across the Federal Government through CISA's Election Security Initiative. CISA and the Election Assistance Commission (EAC) have convened Federal government and election officials regularly to share cybersecurity risk information and to determine an effective means of assistance. Since 2017, the Election Infrastructure Subsector (EIS) Government Coordinating Council (GCC) has worked to establish goals and objectives, to develop plans for the EIS partnership, and to create an EIS Sector-Specific Plan. Participation in the council is voluntary and does not change the fundamental role of state and local jurisdictions in overseeing elections.

CISA and the EAC have also worked with election equipment and service vendors to launch, in 2017, an industry-led Sector Coordinating Council (SCC), a self-organized, self-run, and self-governed council with industry leadership designated by SCC members. The SCC serves as the industry's principal entity for coordinating with the Federal Government on critical infrastructure security activities related to sector-specific strategies. The SCC has helped CISA further its understanding of election systems, processes, and relationships.

CISA, through the Election Infrastructure Information Sharing and Analysis Center (EI-ISAC), now provides threat alerts to all 50 states and more than 2800 local and territorial election offices. In addition, all 50 states, 250 localities, three territories and DC now have intrusion detection sensors. These sensors are operated and monitored by EI-ISAC as part of the Multi-State Information Sharing and Analysis Center's (MS-ISAC) Albert intrusion detection system. DHS shares intelligence and other cyber threat information with EI-ISAC for use in Albert, which assists with identifying specific threats to election infrastructure networks.

For most of the year, COVID-19 has provided an additional layer of complexity to the work of state and local election officials. CISA and the EAC have worked closely with the election community to provide the necessary services and resources throughout the primaries, in the run-up to the general election, and during the voting and post-election periods. At the beginning of the outbreak, the EIS GCC and SCC created a Joint Working Group consisting of government and industry representatives, to analyze aspects of different voting methods and to provide written resources to state and local officials seeking to mitigate exposure to COVID-19 while administering elections. The Joint Working Group has to date produced numerous guidance documents, addressing such issues as voter education about administrative changes and the importance of accurate voter data when expanding absentee voting. CISA has also hosted calls through the spring and summer between the election community and the Centers for Disease Control and Prevention (CDC), the United States Postal Service (USPS), and other relevant Federal partners, to help ensure that election officials have the most up-to-date information and advice from the experts at these agencies regarding COVID-19 response.

CISA continues to build national resilience against foreign influence operations through public education and awareness to help Americans better understand the threat of foreign influence and simple steps they can take to avoid amplifying foreign influence operations. CISA has developed innovative methods to help Americans recognize and avoid foreign disinformation operations targeting our democracy, which includes the #WarOnPineapple campaign to help educate Americans on the tactics of malicious foreign influence campaigns. CISA also coordinates closely with social media platform counterparts to enable election officials to report mis- and disinformation from these platforms.

CISA has worked directly with our Federal, state, and local partners on these and other issues through a number of exercises. In July 2020, we hosted our third iteration of Tabletop the Vote, a nationwide exercise that engaged more than 1,750 participants. The exercise enabled participants to explore and assess issues related to voter confidence, voting operations, and the integrity of elections in response to simulated cyber and physical threats impacting the 2020 election. CISA also works directly with Federal, state, local, and critical infrastructure partners to

exercise their plans and procedures in tailored exercises. In Fiscal Year 2020, we have conducted 22 of these direct partner exercises focused on elections security. These events not only build the capabilities of our partners, but also strengthen the relationships and information sharing among the community to enhance our collective preparedness.

On Election Day, CISA hosted an in-person classified and unclassified operations center, bringing together Federal agencies with private sector organizations, including both major political parties, social media companies, election technology companies, and other organizations. CISA also stood up a virtual National Cybersecurity Situational Awareness Room, an online portal for state and local election officials and their private sector partners to share real-time information and support as needed. CISA will remain in an enhanced coordinated posture until after all election results have been certified and will continue to remain vigilant to protect against attempts by foreign actors to target or disrupt this process.

**Conclusion**

In the face of increasingly sophisticated threats, CISA employees stand on the front lines of the Federal Government's efforts to defend our Nation's government networks and critical infrastructure. The threat environment is complex and dynamic, with interdependencies that add to the challenge. CISA contributes unique expertise and capabilities around cyber-physical risk and cross-sector critical infrastructure interdependencies.

I recognize and appreciate the Subcommittee's strong support and diligence as it works to understand this emerging risk and identify additional authorities and resources needed to address it head-on. We at CISA are committed to working with Congress to ensure our efforts cultivate a safer, more secure, and resilient Homeland through our efforts to defend today and secure tomorrow.

Thank you for the opportunity to appear before the Subcommittee today, and I look forward to your questions.

WRITTEN TESTIMONY

OF

DENIS GOULET

COMMISSIONER OF THE DEPARTMENT OF INFORMATION TECHNOLOGY

STATE OF NEW HAMPSHIRE

AND

PRESIDENT OF THE NATIONAL ASSOCIATION OF STATE CHIEF INFORMATION OFFICERS (NASCIO)

FOR A HEARING ON

"STATE AND LOCAL CYBERSECURITY: DEFENDING OUR COMMUNITIES FROM CYBER THREATS AMID COVID-19"

BEFORE THE

UNITED STATES SENATE

FEDERAL SPENDING OVERSIGHT AND EMERGENCY MANAGEMENT SUBCOMMITTEE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

Wednesday, December 2, 2020

Washington, D.C.

Thank you, Chairman Paul, Ranking Member Hassan and the distinguished members of the Subcommittee for inviting me today to speak on the numerous cybersecurity challenges facing state government that have been amplified during the COVID-19 pandemic. As Commissioner for the Department of Information Technology in New Hampshire and the President of the National Association of State Chief Information Officers (NASCIO), I am grateful for the opportunity to discuss cybersecurity, as well as highlight the vital role that state information technology (IT) agencies have played in providing critical citizen services and ensuring the continuity of government throughout this current public health crisis.

**State Cybersecurity Overview and Challenges**

As President of NASCIO, I am extremely honored to represent my fellow state chief information officers (CIOs) and other state IT agency leaders from around the country here today. While some of my testimony will be based on my experiences as CIO in New Hampshire for over the past five years, I will also be providing the members and staff of the Subcommittee with national trends and data from NASCIO's recently completed 2020 State CIO Survey and the 2020 Deloitte-NASCIO Cybersecurity Study.

It may come as little surprise to you that cybersecurity has remained the top priority for state CIOs for the past seven years. There is certainly growing recognition at all levels of government that cybersecurity is no longer an IT issue; it is a business risk that impacts the daily functioning of our society and economy, as well as a potential threat to our nation's security. The threat environment we face is incredibly daunting with state cyber defenses repelling between 50 and 100 million potentially malicious probes and actions every day. State and local governments remain attractive targets for cyber-attacks as evidenced by dozens of high-profile and debilitating ransomware incidents. The financial cost of these attacks is truly staggering with a recent report from EMSISOFT finding that ransomware attacks in 2019 impacted more than 960 government agencies, educational institutions and healthcare providers at a cost of more than $7.5 billion.

Inadequate resources for cybersecurity has been the most significant challenge facing state and local governments, even prior to the COVID-19 pandemic. The question of why the federal government should be contributing to cybersecurity of the states is straightforward as states are the primary agents for the delivery of a vast array of federal programs and services. I do want to point out that a large majority of state CIO agencies operate on a cost recovery or chargeback model, whereby they bill state agencies for services provided. While this model has its own challenges, half of the states and territories currently lack a dedicated cybersecurity budget and more than a third have seen no growth or a reduction in those budgets. According to our recent national survey, state cybersecurity budgets are typically less than 3 percent of their overall IT budget.

As state CIOs are tasked with additional responsibilities, including providing cybersecurity assistance to local governments, they are asked to do so with shortages in both funding and

cyber talent. Only half of all states have a dedicated cybersecurity budget line item while federal government agencies report cybersecurity funding in the president's budget as a portion of their overall IT spending. This is marginal compared to private industry cybersecurity budgets.

NASCIO has long encouraged state government officials to establish a dedicated budget line item for cybersecurity as subset of the overall technology budget. While the percentage of state IT spending on cybersecurity may be much lower than that of private sector industry and federal agency enterprises of similar size, the line item can help state IT leaders provide the state legislature and executive branch leaders the right level of visibility into state cybersecurity expenses in an effort to rationalize spending and raise funding levels. State legislation could demand visibility into cyber budgets at both the state and individual agency levels. In addition, the Deloitte-NASCIO Cybersecurity study results indicate that federal and state cybersecurity mandates, legislation, and standards with funding assistance result in more significant progress than those that remain unfunded.

**A Whole-of-State Approach**

More than 90 percent of CIOs are responsible for their state's cybersecurity posture and policies. In collaboration with their chief information security officers (CISOs), whose role has expanded and matured in recent years, CIOs have taken numerous initiatives to enhance the status of the cybersecurity program and environment in their states. I believe these initiatives are also fundamentally crucial as Congress considers the implementation of a cybersecurity grant program for state and local governments. Some of these include: the adoption of a cybersecurity strategic plan, the adoption of a cybersecurity framework based on the NIST Cybersecurity Framework, the development of a cyber disruption response plan, obtaining cyber insurance and the development of security awareness training for employees and contractors.

One key initiative is the whole-of-state approach to cybersecurity, which NASCIO has advocated for the past decade. We define the whole-of-state approach to cybersecurity as collaboration among state agencies and federal agencies, local governments, the National Guard, education (K-12 and higher education), utilities, private companies, healthcare and other sectors. By approaching cybersecurity as a team sport, information is widely shared and each stakeholder has a clearly defined role to play when an incident occurs. Additionally, many states who have adopted the whole-of-state approach have created statewide incident response plans.

Crucially, numerous state IT agencies are conducting cyber incident training and incident response exercises with these partners to ensure the ability to quickly operationalize their incident response plans. According to our recent CIO survey, more than 65 percent of state CIOs are either in the process of implementing a whole-of-state approach or have implemented one in their states.

In August 2019, more than two dozen local governments, education institutions and critical infrastructure systems in Texas were struck by debilitating and coordinated ransomware attacks. However, it was the successful collaboration and cooperation among federal, state and local officials – a whole-of-state approach combined with a detailed cyber incident response plan – that prevented these attacks from succeeding. In fact, as Amanda Crawford, Executive Director of the Texas Department of Information Resources (DIR), testified before the Senate Homeland Security and Governmental Affairs Committee in February 2020, all impacted entities were remediated within one week after the attacks.

**State and Local Collaboration**

As the Texas ransomware attacks illustrate, under-resourced and under-staffed local governments continue to remain an easy target for cyber-attacks. Due to the combination of a whole-of-state approach to cybersecurity and the proliferation of numerous high-profile ransomware attacks across the country, state CIOs have significantly increased collaboration with local governments to enhance their cybersecurity posture and resilience. More than 76 percent of CIOs reported increased collaboration and communication with local governments in the last year.

Earlier this year, NASCIO released a research paper with the National Governors Association (NGA) focused on state and local collaboration titled "Stronger Together." As Congress considers the components of a state and local cybersecurity grant program, I would urge you to incorporate some of the conclusions from that paper. This includes encouraging states to continue building relationships with local governments and helping states raise awareness for IT and cybersecurity services offered to local governments. Additionally, Congress should assist state and local governments with more easily purchasing cybersecurity tools and services through existing models at the federal level. Streamlining the procurement of cybersecurity services would also expedite a currently bureaucratic process and result in significant cost savings.

**Partnership with DHS CISA**

In terms of partnerships with federal agencies, I do want to highlight state IT's growing partnership with the DHS CISA. While this relationship is still in its infancy, CIOs and CISOs appreciate the resources provided to state and local governments by CISA in the wake of cyber attacks. NASCIO has supported efforts to more clearly define CISA's roles and responsibilities in assisting state and local governments and has endorsed federal legislation to increase CISA's resources within each state.

In January 2020, NASCIO endorsed **S. 3207, the Cybersecurity State Coordinator Act of 2020**, introduced by Ranking Member Hassan, which would be a major asset to state and national cybersecurity efforts by ensuring greater continuity between the efforts of states and the Federal Government. It would also provide a stronger state voice within CISA, helping them to better tailor their assistance to states and localities.

**Supported Federal Legislation**

I would like to reiterate my appreciation to this subcommittee for its attention to cybersecurity issues impacting state and local governments. The 116th Congress certainly has focused significantly on these issues and introduced legislation endorsed by NASCIO. If passed, these bills would greatly improve the cybersecurity posture for state and local governments by creating new, dedicated funding streams.

As you may know, cybersecurity spending within existing federal grant programs, including the Homeland Security Grant Program, has proven challenging in the face of declining federal allocations, increased allowable uses and a strong desire to maintain existing capabilities that states have spent years building. In fact, less than four percent of all Homeland Security Grant Program funding has been allocated to cybersecurity over the last decade.

These proposed cyber grant programs through legislation introduced during the 116th would provide vital resources for state IT agencies that would prevent my fellow CIOs and I from having to compete against other agencies and states. Ultimately, a specific cybersecurity grant program would allow us to better assist our local government partners and thwart well-funded nation-states and criminal actors that continue to grow in sophistication.

NASCIO supports **S. 1846**, **the State and Local Government Cybersecurity Act**, which would help states access resources, tools, and expertise developed by our Federal partners and national cybersecurity experts. This includes making available to state and local governments the experts at the Department of Homeland Security's (DHS) National Cybersecurity and Communications Integration Center (NCIC) for training and consulting. It would also afford these organizations with greater access to security tools, policies, and procedures to help drive vital improvements.

Additionally, NASCIO worked closely with bipartisan members of the House Committee on Homeland Security on the introduction of **H.R. 5823**, **the State and Local Cybersecurity Improvement Act**, a $400 million annual grant program for state and local governments to strengthen their cybersecurity posture. H.R. 5823 would require grant recipients to have comprehensive cybersecurity plans and emphasizes significant collaboration between DHS Cybersecurity and Infrastructure Security Agency (CISA) and state and local governments.

NASCIO also urges Congress to pass **S. 2749**, **the DOTGOV Act**, which would go a long way in providing greater security assurance for state and local government websites. Nearly twenty years after making the .gov domain available to state and local governments, the vast majority of local governments are still not taking advantage of this trusted domain. As of today, there are only approximately 8.5 percent of all eligible local governments on .gov, allowing cyber criminals to spoof websites and further wage misinformation and disinformation campaigns.

The DOTGOV Act seeks to ease the process for these governments to obtain .gov domain names, providing the sites themselves with greater security and offering greater assurances to

residents that they are, in fact, looking at a government website. The bill also charges DHS with providing information to make the transition to the .gov domain easier and allows the Director of CISA to waive fees related to .gov registration.

**Conclusion**

For more than the past eight months, the COVID-19 pandemic has clearly exacerbated the cybersecurity challenges for state IT agencies. In response to the pandemic, state CIOs and their teams quickly provided a secure remote work environment for more than 90 percent of state employees. Since March, my colleagues and I have rapidly implemented policies on how state employees should use personal devices, patch their systems and ultimately, how to conduct telework safely in this new environment. We have also assisted numerous state agencies to help them improve their technological capabilities and quickly deliver critical services to citizens, including unemployment insurance.

In New Hampshire, I have worked closely with our public health agencies to ensure they have the necessary digital tools for them to improve capabilities in the areas of testing, contact tracing, case management and personal protective equipment (PPE) inventory.

My colleagues and I at the Department of Information Technology have been honored to play a role in fighting COVID-19 in New Hampshire. We have taken on additional responsibilities and incurred new expenses while continuing to face an unrelenting cybersecurity threat environment. I am truly concerned about how crucial IT and cybersecurity initiatives will remain funded in the coming months and years. We all know that states have seen significant declines in revenue and will be forced to make difficult budgetary decisions in the coming years.

As President of NASCIO, I know I speak for all of my colleagues around that country that a federally funded cybersecurity grant program for state and local governments is long overdue. There can be no doubt that state governments need to change their behavior and begin providing consistent and dedicated funding for cybersecurity moving forward. It is my hope that the states will follow the lead of the federal government in this area, especially if grant programs require them to match a portion of federal funds. I look forward to continuing to work with the members of this subcommittee in the creation of a grant program to improve the cybersecurity posture for our states and local governments.

**Washington, D.C. Office**
800 10th Street, N.W.
Two CityCenter, Suite 400
Washington, DC 20001-4956
(202) 638-1100

**Testimony**

**of the**

**American Hospital Association**

**for the**

**Subcommittee on Federal Spending Oversight and Emergency Management**

**of the**

**Committee on Homeland Security and Governmental Affairs**

**of the**

**U.S. Senate**

**December 2, 2020**

Chairman Paul, Ranking Member Hassan and members of the Subcommittee, my name is John Riggi and I am the Senior Advisor for Cybersecurity and Risk at the American Hospital Association (AHA).

On behalf of our nearly 5,000 member hospitals, health systems and other health care organizations, our clinician partners – including more than 270,000 affiliated physicians, 2 million nurses and other caregivers – and the 43,000 health care leaders who belong to our professional membership groups, the AHA thanks the Subcommittee for the opportunity to testify on, and your interest in, the important issue of cybersecurity threats faced by hospitals, health systems and the health care provider field. Now more than ever, we all realize how vital hospitals are to the nation's critical infrastructure and how important they are to our communities' health and safety.

Today, within the context of the COVID-19 pandemic, I will discuss increased incidences of cyber threats toward hospitals and health systems, the resulting, unique challenges confronting the health care sector, and what the federal government can and must do to help ensure appropriate mechanisms are in place to share threat information and defend the nation's hospitals and health systems from cyber attacks.

The AHA has a unique national perspective on these issues, stemming from communications with thousands of trusted hospital leaders across our field and robust interaction with federal agencies. We are privileged to serve as an effective platform to facilitate communication and cooperation between the government and health care in our common interest to defend the field and the nation against cyber attacks. We also welcome the opportunity to inform the work of this committee in this capacity and stand ready to assist as needed.

Hospitals and health systems appreciate the recent efforts by federal agencies such as the Department of Homeland Security (DHS), Cybersecurity and Infrastructure Agency (CISA), Federal Bureau of Investigation (FBI), Department of Health and Human Services (HHS), National Security Agency (NSA) and United States Secret Service (USSS) to disseminate cyber threat intelligence and respond to cyber attacks targeting health care during this pandemic.

The most recent national threat advisory of imminent ransomware attacks targeting hospitals, issued on Oct. 28, 2020, by CISA, FBI and HHS[1], was a good example of timely and actionable intelligence being shared by the government in a coordinated effort across agencies.

**THREATS TO HOSPITALS AND HEALTH SYSTEMS**

Unfortunately, the aforementioned alert, CISA AA20-302A, is also a good example of the tremendously increased cyber risk faced by hospitals emanating from foreign cyber criminals and spies seeking to take advantage of hospitals that labor under the strain of caring for COVID-19 patients. The alert stated that "CISA, FBI, and HHS have credible information of an *increased and imminent cybercrime threat to U.S. hospitals and healthcare providers,"* which remain ongoing as of this date. This threat is very telling as to the nature of the cyber adversaries we face. The adversaries seek to exploit the global pandemic for financial gain, aware that ransomware attacks on hospitals disrupt patient care services and risk patient safety.

This ongoing threat is the most significant and widespread cyber threat to face hospitals since the global WannaCry ransomware attacks in 2017 perpetrated by the North Korean government.[2]

Hospitals, and the overall health care sector, have long been heavily targeted by cyber adversaries due to the various critical data sets in their possession that cyber criminals can easily monetize. Yet, during the pandemic, we have witnessed an increase in the frequency, severity and sophistication of cyber attacks on hospitals and health systems. The pandemic, therefore, has led to a cyber "triple threat" for hospitals and health

[1] https://us-cert.cisa.gov/ncas/alerts/aa20-302a
[2] https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and

systems: an expanded attack surface; increased cyber attacks of all types; and fewer available resources to bolster cybersecurity defenses.

**Expanded "Attack Surface"**

In preparation for and response to COVID-19, the health care sector rapidly deployed and expanded network- and internet-connected technologies and services to a scale never experienced in health care.

For example, technologies for telehealth, telemedicine, telework and cloud based services were quickly adopted and expanded due to clinical and operational necessity at the encouragement of federal and state governments. Many hospitals and health systems have also expanded, within care units, remote monitoring of ventilators and other medical devices. These actions were taken to improve efficiency and to preserve precious personal protective equipment (PPE) in departments whose focus is on caring for COVID-19 patients.

The expansion of network-connected technologies and health devices has resulted in an exponential expansion of network access points. For cyber criminals, this has translated into a greatly expanded "attack surface." In other words, there are now many more opportunities to exploit technical vulnerabilities and penetrate hospital networks. Telehealth has emerged as a lifeline for many patients during the pandemic and is one that must be sustained. Such patients rely on the access provided through telehealth; cybersecurity is, at its core, a necessary element of patient safety for hospitals and health systems.

**Increased Cyber Attacks**

Cyber adversaries have launched relentless attacks on hospitals and health systems. Hacking incidents of all types targeting hospitals and health systems increased significantly throughout 2020. According to data from the HHS Office of Civil Rights (OCR) Breach Portal on 11/27/20[3] for the three month period between Sept. 1 and Nov. 27 of this year, there were 162 active and resolved hacking incidents affecting 12.6 million individuals. Comparatively, there were 218 active and resolved hacking incidents for the eight-month period between Jan. 1 and Aug. 31, affecting 7.3 million individuals.

At the onset of the COVID-19 pandemic, there was a dramatic increase in phishing email campaigns directed toward the health care sector and the general public. Social engineering techniques, such as COVID-19-themed phishing emails containing malware and links to malicious sites, increased by nearly 700%[4] worldwide by some accounts. Such emails are sent under the guise of providing important COVID-19 information. They make fake promises; one example might offer for sale equipment made scarce by the public health emergency, such as N95 masks and lifesaving ventilators. Instead these emails are laden with malware and malicious links.

[3] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

[4] https://blog.barracuda.com/2020/03/26/threat-spotlight-coronavirus-related-phishing/

Phishing remains the primary method to introduce malware and ransomware into hospitals, requiring dedicated, diligent hospital staff to monitor and educate workforces that are already strained due to the pandemic. Phishing emails are used by criminals not only to launch cyber attacks, but to also perpetrate fraud and steal funds, again using COVID-19 as their entry point. For example, it is common for hospitals and health systems to receive emails promising to supply scarce PPE in exchange for a down payment; they later discover that the PPE was counterfeit and of inferior quality, or perhaps never existed.

Foreign-based cyber criminals have taken advantage of the pandemic to steal data and threaten patient care. According to U.S. government alerts, highly sophisticated foreign intelligence services and military units from China, Russia and Iran have launched cyber campaigns targeting health care to steal COVID-19-related research, such as treatment protocols and vaccine data. In a disturbing trend, hostile foreign intelligence services are working in conjunction with cyber criminals (whose hacking capabilities and access are most useful to them) to target a wide scope of networks, including those related to health care.

As evidence of this phenomena, on Sept. 16, 2020 the Department of Justice (DOJ) stated in regard to the indictment of two Iranian hackers, "Unfortunately, our cases demonstrate that at least four nations — Iran, China, Russia and North Korea — will allow criminal hackers to victimize individuals and companies from around the world, as long as these hackers will also work for that country's government..."[5] In another example from Sept. 16, DOJ stated that, "the Chinese government tolerated the defendants' criminal activity because those defendants were willing to work on behalf of the Chinese intelligence services."[6]

Data breaches through businesses associated with hospitals and health systems, including third-party vendors storing sensitive patient information, also continue to be a problem. According to the HHS Office of Civil Rights (OCR), this continues to be a significant factor in large data breaches impacting millions of patients.

Ransomware attacks are a considerable concern, especially for a hospital overloaded by caring for COVID-19 patients. Such an attack could interrupt patient care, or worse, shut down operations at the facility, thereby putting patient lives, and the community, at risk. This is what happened this past March 12 to Brno University Hospital in the Czech Republic. The hospital, which is among the Czech Republic's largest coronavirus testing centers, was forced to redirect patients to other hospitals. At the same time, another facility in the city of Brno, the Children's and Maternity Hospital, was also hit. There have been recent domestic examples of ransomware attacks on hospitals and health systems which result in the interruption patient-care services. Ransomware attacks on

[5] https://www.justice.gov/opa/pr/two-iranian-nationals-charged-cyber-theft-campaign-targeting-computer-systems-united-states

[6] https://www.justice.gov/opa/speech/remarks-deputy-attorney-general-jeffrey-rosen-announcement-charges-and-arrests-computer

hospitals can result in the cancelation of routine appointments and surgeries, delays in treatment, denied access to electronic medical records at critical moments – including drug allergy information – and the diversion of ambulances carrying trauma patients to emergency departments that may be further away.

**Resource Constraints**

The third threat hospitals and health systems are experiencing are the human, financial and technical cybersecurity resource constraints due to reduced hospital revenue. The AHA released a report in June which estimated total losses for the nation's hospitals and health systems to be at least $323.1 billion in 2020. Reduced revenue due to canceled elective surgeries and patients' reluctance to seek non-COVID-19-related medical treatment during the pandemic has significantly decreased hospitals' and health systems' financial resources, leaving limited funds available to enhance network defenses and to recruit and retain cybersecurity professionals. Hospitals' cybersecurity workforce issues are exacerbated by the fact that there is already a shortage of professionals capable of meeting the demand for cybersecurity talent across all industries and government; furthermore, the health care field often has more limited budgets for these personnel than other sectors of the economy.

In summary, hospitals and health systems face a perfect storm of factors leading to expanded cyber threats and risks– an expanded attack surface, increased frequency of cyber attacks of all types and constrained resources available to bolster cybersecurity defenses. Ultimately, the issues we are discussing today are key factors for patient safety and patient access.

**EXPAND PUBLIC-PRIVATE PARTNERSHIPS AND CROSS-INDUSTRY EFFORTS**

An increase in classified and unclassified threat information sharing through appropriate channels is an important step toward helping hospitals and health systems defend themselves. Although DHS, CISA, the FBI, HHS and the U.S. Secret Service have done a commendable job in sharing threat information with the health care field and producing timely and high quality joint intelligence products, more needs to be done.

Threat information must be coordinated among the various agencies, centralized, disseminated consistently and made available in both narrative and automated fashion. Further, it must be *free* – entirely absent of fees paid to any cyber threat information-sharing entity. It is especially important that technical indicators of compromise (IOCs), which are the lengthy and voluminous technical malware signature codes, be automated and made readily accessible to all trusted health care entities. This was the intent of the Cybersecurity Information Sharing Act of 2015.

Timely dissemination of threat intelligence in an automated fashion and other joint efforts can play an important role in derailing cyber attacks; it can also help organizations recover and resume operations more quickly in the event of an attack's

success. Both of those outcomes reduce the financial incentive for cyber criminals to carry out ransomware attacks.

The AHA, along with the Healthcare-Information Sharing and Analysis Center (H-ISAC), the Health Care Sector Coordinating Council (HSCC) and the HHS-sponsored Health Care Industry Cyber Security Task Force, has urged more public-private partnerships to improve cyber security in a "whole of nation" approach to defend against cyber threats.

In the realm of cyber defense there is no competitive advantage between organizations, especially in health care. All face the same threats and, thus, the same potential consequences. As a result, all have the same incentive to freely exchange threat information for the common defense as well as for the defense of public health and safety.

**UNIQUE CHALLENGES FOR THE HEALTH CARE SECTOR**

Health care is the only economic sector that possesses a combination of highly targeted data sets such as personally identifiable information, payment information, protected health information, business intelligence, intellectual property related to medical research and innovation – including genomic studies related to the development of precision medicine – and, as a critical infrastructure sector, national security information related to emergency preparedness and response in times of national crisis or war.

Each one of these data sets is heavily targeted by cyber adversaries. Individually, these data sets are highly valuable to the cyber adversary; together, they become exponentially valuable.

Also, health care records continue to command a premium price on the dark web because they have enduring value to cyber adversaries. In other words, unlike credit card numbers, one cannot cancel their blood type or a medical diagnosis. Stolen health care records may be the source of repeated health care fraud, used to fund more serious crime, including violent crimes by foreign gangs or be exploited on an ongoing basis for intelligence purposes by a nation-state.

**VICTIMS OF CYBER ATTACKS SHOULD BE PROVIDED ASSISTANCE, NOT ASSIGNED BLAME**

Despite complying with rules and implementing best practices, hospitals and health care providers will continue to be the targets of sophisticated attacks, some of which will inevitably succeed. The government often repeats the phrase, "It's not a matter of if, but when," in regard to an organization becoming a victim of a cyber attack. Organizations that are victims of breaches should be treated as victims of crime, an approach that has been codified in Presidential Policy Directive/PPD-41: United States Cyber Incident Coordination.

Unfortunately, the federal government's approach toward victims of cyber attacks is sometimes inconsistent across agencies and often counterproductive.

For example, federal law enforcement agencies often request and *need* the cooperation of victims of breaches to further their investigations and disrupt the threat to the nation. Simultaneously, a hospital or health system may be the subject of an onerous and adversarial investigation by the HHS Office of Civil Rights; this can be disruptive and have a chilling effect in regard to the government's interest and efforts to obtain victims' cooperation with federal law enforcement.

The victims of attacks should be given support and resources; attackers are the ones who should be vigorously investigated and prosecuted. Even if an organization were the victim of a cyberattack, it does not mean that the organization itself was in any way at fault or unprepared. Similarly, a breach does not necessarily equate to a Health Insurance Portability and Accountability Act (HIPAA) Security Rule compliance failure. Instead, successful attacks should be fully investigated, and the lessons learned should be widely disseminated to prevent the success of similar attacks in the future. President Obama signed into law the Consolidated Appropriations Act, 2016, Public Law 114-113, which included the Cybersecurity Information Sharing Act of 2015 (CISA). Recognizing the seriousness of the cyber threat facing the nation and the private sector, Congress established through CISA a voluntary cybersecurity information sharing process that encourages public and private sector entities to share cyber threat indicators and defensive measures while protecting privacy and civil liberties.[7]

To encourage this sharing, CISA includes certain safe harbor protections from civil, regulatory and anti-trust liability for sharing conducted in accordance with CISA.

Since the passage of CISA, the cyber threats against health care and the nation have increased significantly. Every hospital and health system in America places utmost importance on protecting the security and privacy of the patient data. However, as the government publicly acknowledges, no organization is or can be completely immune from cyber attacks. Regardless of the amount of human, technical and financial resources devoted to cybersecurity by any organization, cyber risk to the organization can be mitigated, but never eliminated.

We recommend that, given the increased cyber threat environment and attacks specifically targeting hospitals and health systems, along with resource constraints imposed upon hospitals and health systems in response to COVID-19, *additional safe harbor protections from civil and regulatory liability be provided to hospital and health system victims of cyber attacks*. We welcome the opportunity to explore this possibility with the committee.

**DEFEND FORWARD**

[7] https://www.federalregister.gov/documents/2016/06/15/2016-13742/cybersecurity-information-sharing-act-of-2015-final-guidance-documents-notice-of-availability

A ransomware attack on a hospital crosses the line from an economic crime to a threat-to-life crime; such attacks should therefore be aggressively pursued and prosecuted as such by the federal government. We use the term "prosecuted" in all senses of the definition related to the government's capabilities and authorities, which include and extend beyond the government's law enforcement authorities found under United States Code (USC) Title 18.

This situation is analogous to the attacks on our nation on Sept. 11, 2001. In the aftermath of those attacks, all of the government's capabilities were brought to bear to detect, deter and disrupt terrorist organizations – including those operating outside of U.S. borders that were beyond the reach of the FBI. In its whole-of-government approach, the U.S. leveraged its military authorities under USC Title 10 and its intelligence authorities under USC Title 50 to protect the homeland from foreign threats operating from safe harbors provided by hostile nation states and non-cooperative foreign jurisdictions.

The laws typically used to prosecute cyber crimes are not commensurate with the level of harm cyber attacks on hospitals can cause. For example, USC Title 18 §1030 is the Computer Fraud and Abuse statute that is used to prosecute hacking activity and other crimes related to computers. It carries a maximum sentence of 20 years in prison. But, due to sentencing guidelines related to this statute, sentences meted out are often far less than 20 years. This is not a strong enough deterrent for an international ransomware criminal who could be reaping millions of dollars in illegal profits along with a low probability of being apprehended.

We do not need more laws to improve legal deterrence for cyber crimes against hospitals. Rather, we should make better use of the laws and other law enforcement tools that are already available.

For example, USC T18 §1030 is most appropriate for prosecuting some ransomware attacks, but can be made more powerful when combined with, or replaced with, alternate prosecution strategies, which include other federal statutes covering Racketeer Influence and Corrupt Organizations, money laundering, commercial extortion, homicide and even terrorism. These additional crimes carry far more serious penalties that are more consistent with the threat-to-life element presented by disruptive cyber attacks against hospitals.

The U.S. response to cyber attacks against health care infrastructure should expand beyond heavy reliance on USC Title 18 for criminal investigation and prosecution. The authorities provided under USC Titles 10, 31 and 50 should all be invoked as necessary to provide more effective and robust options to deter and disrupt foreign-based adversaries that attack U.S. hospitals and health systems.

Title 31 allows the Treasury Department, through the Office of Foreign Asset Control (OFAC), to put financial sanctions on foreign entities that have conducted or facilitated

cyber attacks against U.S. organizations. OFAC sanctions also make it a crime for any other entity or person to conduct business with an OFAC-designated entity.

Titles 10 (military authorities) and 50 (intelligence authorities) can improve domestic cyber defenses by putting the U.S. on the offensive. They could be invoked to take an "active" or "forward" defensive posture to proactively disable and disrupt foreign-based cyber threats. The vast resources, knowledge and capabilities of the U.S. Cyber Command, National Security Agency (NSA), CIA and the rest of the intelligence community are unmatched and could be used to augment and support law enforcement actions, in sequenced and coordinated operations as part of an overall national strategy, as was done in the during the war on terrorism in the aftermath of 9/11.

In October 2020, U.S. Cyber Command conducted offensive cyber operations aimed at disrupting the Trickbot botnet used to distribute ransomware[8] and the FBI indicted six Russian military intelligence officers[9] implicated in distributing destructive malware. This is an excellent example of a unified, coordinated government approach to the global cyber threat, utilizing a combination of elements of national power.

**COORDINATED GOVERNMENT SUPPORT AND PARTNERSHIP ARE KEY TO STOPPING CYBER CRIME**

Despite hospitals' concerted attempts to secure their cyber ecosystems, individual efforts to secure systems are insufficient to prevent all attacks. The Trump Administration has used executive orders to name 16 critical infrastructure sectors – including health care and public health – deemed essential to the security of the nation and directed federal agencies to prioritize securing federal systems. HHS is designated as the liaison for the health care sector. More broadly, the FBI has been designated as the lead authority on investigating cybercrime. Other agencies, including the Department of Homeland Security and the Secret Service, also play key roles in combatting cybercrime and providing guidance. Coordination across these federal resources is critical to ensuring the wide, effective and timely sharing of threat intelligence and defensive strategies. In addition, these agencies must be given the resources to not only respond to attacks, but also help vulnerable health care targets prevent attacks from occurring or succeeding.

We have seen that the most effective response by the government to aid health care victims of cyber attacks is a consistent unified approach in which DHS, FBI and HHS respond in a timely and coordinated manner. *A call to one should be "a call to all."* The National Cyber Investigative Joint Task Force (NCIJTF), which also encompasses intelligence community and Department of Defense assets, may be the platform to further refine and enhance inter-agency coordination and response efforts.

---

[8] https://www.washingtonpost.com/national-security/cyber-command-trickbot-disrupt/2020/10/09/19587aae-0a32-11eb-a166-dc429b380d10_story.html

[9] https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and

As referenced above, the CISA Act provided a mechanism for sharing information among private-sector and federal government entities and provides a safe harbor from certain liabilities related to that information sharing. Information sharing allows organizations to stay ahead of emerging cybersecurity risks and contribute to our collective knowledge of threats. However, the goals of information sharing have yet to be fully realized. Expedited, tailored and automated cyber threat information sharing on a regular cadence from the federal government would benefit all health care and public health organizations. Providers need actionable information that identifies specific steps they can take to secure against new threats. Large volumes of more generalized information can prove challenging to interpret and may even become a distraction.

HHS also is directed under the Cybersecurity Information Sharing Act to work with the private sector and other federal agencies to establish voluntary, consensus-based best practices. While the federal government is working to provide additional educational and other resources to the health care field, more action is needed to address the cybersecurity challenges facing all sectors. As a nation, we must bolster the security of our cyber ecosystem, not just place the burden on individual institutions. Indeed, the magnitude of the challenges and the growing sophistication of the attacks suggest that the federal government must provide additional nationwide resources. These include efforts to:

- develop and disseminate coordinated national defensive measures, including leveraging national technical defenses which are used to protect government agencies;
- strengthen and expand our cybersecurity workforce through grant programs and retraining efforts, perhaps with a particular focus on the retraining of veterans;
- identify and disrupt bad actors;
- increase the consequences for those who commit attacks; and
- identify and support best practices by the private sector.

**CONCLUSION**

Hospitals and health systems, and the patients they care for every day, are heavily targeted by cyber adversaries, including sophisticated nation-states. They have made great strides to defend their networks, secure patient data, preserve health care services' efficient delivery and, most importantly, protect patient safety. However, our field cannot do it alone. Hospitals and health systems need more active support from the government to defend patients from cyber threats.

Conversely, the federal government cannot protect our nation from cyber criminals alone either – they need the expertise and exchange of cyber threat information from the field to effectively combat cyber threats.

What is truly needed is close cooperation between the government, the health care sector and all critical infrastructure via a formal exchange of cyber threat information and combined cyber defenses – truly a "Whole of Nation Approach."

HARTFORD
PUBLIC SCHOOLS

**Senate Testimony**
**Hartford Public Schools/City of Hartford Cyberattack**
**Dr. Leslie Torres-Rodriguez, Superintendent Hartford Public Schools**
December 2, 2020

Good Afternoon Senator Hassan and Senators of the Committee,

I am Dr. Leslie Torres-Rodriguez, the proud Superintendent of Hartford Public Schools. Hartford Public Schools is the third-largest school district in Connecticut with approximately 18,000 students. I appreciate your invitation to address the committee and answer questions regarding the cyberattack on Hartford Public Schools and the City of Hartford that occurred in September.

The cyberattack had extremely disruptive effects on our school system, students, and staff. We were forced to postpone our first day of school on September 8, following months of intense planning for in-person learning amidst the COVID-19 pandemic. While our beautiful and capable students have been attending school either in-person or online for nearly three months now, we are still repairing and recovering from the lingering effects of the attack.

Hartford Public Schools and the City of Hartford were informed by our shared IT department, Metro Hartford Information Services, that in the early morning hours on Saturday, September 5, we experienced a severe cyberattack. Specifically, a ransomware attack, which aims to take control of targeted servers and sell access back to the owner. The attack was unsuccessful overall because Metro Hartford Information Services regained control of its servers without complying with the attacker's demands, thanks to recent cybersecurity investments and quick work by the MHIS team. Based on initial analysis by the Connecticut National Guard and the Federal Bureau of Investigation, the attack was likely conducted by a highly sophisticated actor, and so in one sense we are fortunate that we avoided the worst-case scenario.

The HPS Team, Metro Hartford Information Services, and the Mayor's office worked late into the night on Labor Day and into the early hours on Tuesday, September 8 to ensure that Hartford Public Schools' critical systems were restored so that the first day of school could proceed. Our Student Information System was restored around midnight but as of 3 AM, our transportation system was still not accessible. Our transportation company and schools had no access to the student bus schedules. Around 4 AM, I made the difficult call to postpone our first day of school.

Fortunately, we were able to get our transportation system online by the evening of September 8 and we opened our schools for the first time since March on Wednesday, September 9. However, two

HARTFORD
PUBLIC SCHOOLS

weeks later, our systems were still not yet fully operational and the costs to address this problem, financially and in resources and staff time, have been significant.

While we have regained control of our servers and data, preventative measures are ongoing and present significant challenges to getting back to normal operations. For example, all our servers needed to be taken offline and reimaged or restored from backups. The total amount of information that needed to be restored is over 70 terabytes across the City and school system, which is a massive amount of information.

Additionally, every computer that had connected to the district network before the attack – just before the start of the school year – had to be individually restored to factory settings before reconnecting with the network. This required a very fast deployment of new laptops to hundreds of staff members, which depleted our stock of laptops to provide to students at a critical time in the school year. While we had ordered new laptops with the intention of ensuring every student had a district device at the start of the school year, that plan was set back because of the cyberattack. This was an especially difficult consequence of this attack as many of our students are participating in online learning from home and need a reliable device to engage in their schoolwork. These preventative measures impeded our ability to operate normally, and for teachers to provide student instruction, impairing even basic functions like scanning and printing.

I am proud of the work done by our IT team, city officials, and district administration, and thankful for the investigative actions and support from the Connecticut National Guard and the FBI. However, we need to protect our critical infrastructure by preventing such attacks in the future.

Thank you again Senator Hassan for inviting me to testify today before this sub-committee on this important issue. While this attack was unexpected and damaging in many ways, I am grateful for the way our local, state, and federal agencies collaborated to address the cyberattack and assisted with the restoration efforts. We are all committed to serving our constituents in the best way possible

I would be happy to answer any questions you may have.

Dr. Leslie Torres-Rodriguez
Superintendent
Hartford Public Schools

**Prepared Written Testimony of Bill Siegel, CEO and Co-Founder of Coveware Inc.**

**Federal Spending Oversight Subcommittee of the Committee on Homeland Security and Governmental Affairs**

*State and Local Cybersecurity: Defending Our Communities from Cyber Threats Amid COVID-19*

Wednesday, December 2nd 2020

**Table of Contents:**


| | |
|---|---|
| **Background on Coveware** | **2** |
| **Profile of a Typical Ransomware Attack** | **2** |
| **Background on the Cyber Extortion Industry** | **3** |
| **The Economics of a Ransomware Attack** | **4** |
| **The Role of the Private Cybersecurity Industry** | **7** |
| **How to Reduce Exposure to Ransomware Attacks and Data Breaches** | **8** |
| **Conclusions** | **10** |
| **Appendices** | **11** |

# Background on Coveware

Coveware is a boutique cyber incident response firm that focuses on helping organizations and enterprises through cyber extortion events. Since founding in 2018, Coveware has handled over 2,000 cyber extortion incidents, the majority of which have involved ransomware. The firm's main area of expertise is focused on negotiating with threat actors on behalf of our clients that face extortion demands, and navigating the technicalities of restoring data that has become encrypted. We work alongside privacy attorneys, forensic investigators, restoration firms, and cyber insurance companies and are a member of the No More Ransom Project. Our position during these incidents has provided us with a perspective which has shaped our opinion on ransomware and how to reduce the prevalence of it.

One of the central ways that we aim to fix this problem is through the collection of data. In order to solve any large problem, we first need to understand the facts. With ransomware, there are very few static pools of hard data collected first hand from actual incidents. One of the central reasons we founded Coveware was to change this. We collect a large cohort of data from every case we manage. The data exhausted from the incidents we manage is used for 3 principal activities:

1. To build reporting and analytics that help us navigate future incidents on behalf of our clients.
2. To publish research and reporting about the trends and patterns of cyber extortion attacks, so that readers can learn and hopefully secure their networks.
3. To assist law enforcement investigations of these crimes. We provide law enforcement agencies (principally in the U.S. but also abroad) with a flat file of hard data each quarter. This data augments active investigation into the criminal groups that carry out these attacks.

There are actually a surprisingly small group of ransomware actors that are active at any given time (see Appendix A). Year over year, the composition can change, but week over week, it is typically no more than a dozen variants or groups. These groups use the same repetitive tactics over and over again on successive victims. Why the repetition? If it works and is profitable, there is no reason to change. These are economically rational behavioral traits.

**Profile of a Typical Ransomware Attack**

A typical ransomware attack involves three distinct phases:

1. **Gaining persistence:** A threat actor gains access to the network of an organization. There are several common vectors through which persistence on the network is

achieved (to be discussed later). Regardless of the means by which access is achieved, threat actors will typically elevate themselves to administrative user privileges, allowing them to move freely through the network and control critical systems like domain controllers, anti-virus protection, endpoint protection, authentication, and the back-up systems. During this phase, the actor may attempt to steal banking passwords (so they can be monetized separately) and exfiltrate sensitive data (for further sale to third parties or to add leverage in the extortion). They will map the network and develop a plan to encrypt it.

2. **Detonation:** After sufficient time surveilling and exfiltrating data, the last step is the detonation of the ransomware. The threat actors will turn off antivirus and endpoint protection, which essentially cuts the alarms that would otherwise alert the company. They will delete or encrypt the organization's backup systems. This cripples the company's ability to restore their network quickly. Finally the threat actors will fully encrypt the primary servers and computers of the company. Once the encryption is finished, ransom notes are left on every machine of the organization. They then wait to be contacted.
3. **Extortion:** If the organization has not properly segmented or air gapped their backups, they are effectively crippled. The organization's email is likely inoperable. Their website may be down. Enterprise Resource Planning application systems that control billing, payroll, shipping and other critical functions may be crippled, and phone systems may also be down. Most organizations have to resort to some form of paper and pencil operations if they are truly crippled to this extent. If the degree of interruption threatens the viability of the company, they face two terrible choices: i) choose to lose their customers, dismiss their employees and possibly close their company, or ii) negotiate and pay the ransom demanded by the threat actors. This is the exact choice thousands of organizations are faced with every year. When victims choose to pay a ransom in cryptocurrency to the threat actor, the threat actor may provide a decryption key, though the efficacy of the decryption key can vary between threat actor groups as does the likelihood of receiving the key.

A larger schematic of a typical ransomware attack is provided in Appendix B.

# Background on the Cyber Extortion Industry

The common perception of these attacks is that victims are the *targets* of individual threat actors. Coveware believes this is a dangerous misconception, and that resetting this perception is a fundamental step towards becoming safer. We believe that every computer, on every network that is connected to the internet is a target. The only thing that determines who actually gets targeted and attacked is the relative economics between comparable targets.

Financially motivated cyber criminals run their own operations like businesses. Their operations coordinate and transact with other specialized groups within the cyber extortion industry just like

in any other legitimate industry or market. The groups that conduct ransomware attacks are separate and unique from groups that perform other critical functions. Some groups focus further up the supply chain and are more akin to raw materials producers. These groups actually construct the malware and ransomware code, but don't carry out attacks. There are other groups that specialize in gaining access or persistence. These groups collect stolen credentials, which they then sell to other groups. There are groups that specialize in running elicit dark marketplaces or forums. These forums serve as trading, logistics and communications outposts. The moderators of these forums can serve as escrow agents for goods and payments, and also enforce rules or resolve disputes. There are groups that specialize in the exfiltration and storage of data. Other groups specialize solely in the deployment of ransomware and extortion. Lastly, there are groups that specialize solely in the cash-out process and laundering of extortion proceeds.

All of these components work together cohesively. The industry is globally distributed, well financed and highly profitable. As we can see, this industry has all the trappings of a mainstream legitimate industry. There are raw materials, refined materials, distribution, logistics, finance, communications, and rules. Reputation also matters greatly in this industry even though its participants are largely anonymous to each other. Also, like any other for-profit industry, economics matter. We make this point because in our experience, the power laws of economics tend to be the most effective way to influence the direction of the industry. Active prevention and aggressive pursuit of criminals by law enforcement will never have substitutes, but are dependent on resources. Applying pressure to the economics of the cyber extortion industry is, in Coveware's view, the best way to curtail its growth and corresponding impact to our Nation's public and private organizations.

## The Economics of a Ransomware Attack

Following the three steps of a ransomware attack, we can illustrate the basic economics by breaking down the associated costs and expected proceeds.

1. **Gaining persistence:** The MOST common way that ransomware attacks occur is through compromised credentials to servers configured for remote access or Remote Desktop Protocol ("RDP"). There are groups, separate and apart from ransomware actors, that specialize in harvesting hundreds of thousands of stolen credentials from millions of exposed servers. The purchase of a set of credentials to a compromised RDP machine can be as inexpensive as $50 U.S. dollars.
2. **Detonation:** On a small network, there is little surveillance that needs to be done, so an actor may spend as little as a few hours on the network deploying the ransomware. For the sake of the exercise, let's assume this threat actor could earn $50 per hour elsewhere, and they spend 6 hours prepping the network for detonation. The total cost of

the actor's time is $300.

3. **Extortion:** The average ransom paid in Q2 of 2020 was $178,000 (See Appendix C).

**Economic Arithmetic:**

Total costs: $350
Total proceeds: $178,000
Total Profit: $177,650

Not all attacks are successfully monetized by the actor. Some companies are able to rebuild. Some companies are able to restore from backups. If we factor the total proceeds by a conversion rate of 25% (meaning they only get paid in 25% of the attacks they carry out, our economics are:

Total costs: $350
Total proceeds: $44,500
Total Profit: $44,150

The threat actors profit margin is over 99% (this is before cashout, which may reduce total proceeds through the laundering process). They probably invested a grand total of 12 hours in the attack across all phases. They have also taken virtually NO risk . All activity was conducted remotely over the internet and via proxies. The extortion negotiation was done over encrypted email or TOR chat service that is untraceable. The proceeds of the extortion are in cryptocurrency and may be moved anonymously through well established cash out channels.

***The current profit margins of the cyber extortion industry is THE FUNDAMENTAL problem we need to address.***

The cyber extortion industry is in a state of wild disequilibrium that favors the threat actors. Economics 101 predicts that this industry will continue to expand until the profitability decreases. This is why ransomware and cyber extortion attacks are proliferating.

The damage to the victim is not just the cost of the extortion though. Business interruption costs can be 5-100x larger than a ransom and can bankrupt a business as well. The cost of the interruption is where the economic pain inflicted on the U.S. economy is really felt. The median victim of a ransomware attack in Q2 of 2020 had less than 100 employees. Small businesses are the largest employer of our citizens and the backbone of the U.S. economy. For most of these companies, the question is when, not if, they will become a victim. Most do not believe they are targets.

**Socio-Economic Enablers of Cyber Extortion Industry Growth**

There are further socio-economic enablers that have propelled this industry into growth. In

certain CIS and Eastern European states, there are large populations of STEM educated, working age individuals. They do not have legitimate employment prospects that can provide the financial earnings they desire. Accordingly, they participate in the cybercrime industry to pay their bills and feed their families. The jurisdictions where these populations live are generally beyond the reach of western law enforcement. Additionally, the capital that is returned to the local economies as a result of the cybercrime industry is substantial. These illicit proceeds support legitimate pillars of these local economies such as consumer goods spending and housing. The governments of these jurisdictions are therefore not particularly incentivized to curtail this criminal activity given the support it provides to the local economy. (source: "Industry of Anonymity: Inside the Business of Cybercrime," by Jonathan Lusthaus and "The Criminal Silicon Valley Is Thriving, New York Time Opinion by Jonathan Lusthaus 11/29/2019)

**Technological Enablers of Cyber Extortion Industry Growth**

As this industry has grown, it has also created innovations which allow for the participation of non-technical actors. One innovation of particular concern is known as Ransomware-as-a-Service (RaaS). As the name denotes, RaaS lowers the barrier to entry by automating many of the technical aspects of staging an attack. There are groups that provide RaaS kits, which are simple paint-by-numbers programs. These RaaS kits, along with written playbooks for non-technical actors, make staging an attack easy for non-technical individuals (see Appendix E). A new entrant to the cyber extortion industry can procure a RaaS kit for free, provided they split the extortion proceeds with the developer of the kit. The distributor then uses the RaaS kit in the same 3-step process described above, with similar economic outcomes. By enabling non-technical actors to become distributors of ransomware, the available population of willing participants is dramatically increased. This innovation has lowered a major barrier to entry. Whereas previously, an actor needed:

1. Technical capability necessary to carry out an attack
2. Financial motivation in excess of fear of criminal consequences
3. Access to the tools of the trade

Now actors no longer need technical skills, and access to tools has been made easy. The average dark marketplace has more available SKU's than a typical Home Depot (38,000+), the most commonly used of which are free.

1. ~~Technical capability necessary to carry out an attack~~
2. Financial motivation in excess of fear of criminal consequences
3. ~~Access to the tools of the trade~~

Consequently, the ONLY remaining barrier to entry is having enough financial motivation to overcome fear of the consequences. Violence in the cyber crime industry is extremely rare and almost a non-issue, especially as compared to other illicit industries such as narcotics or traditional organized crime. When set against the backdrop of a global pandemic and its economic consequences, it is clear why every day more and more people tip into participation in

this industry.

This is a frightening picture of what awaits us if the unit-economics of cybercrime remain in disequilibrium. As long as the risk is low, the return is high and the addressable market of hungry participants is growing, this industry will continue to grow and the volume of attacks against organizations and enterprises in the U.S. will continue to rise.

## The Role of the Private Cybersecurity Industry

Private security firms and services to enterprises can play an important role in applying pressure to the economics of the cyber extortion industry. Relative safety from these attacks is a function of resources, and there are too many organizations and enterprises that operate below the cyber security poverty line. This intangible line separates those that can afford to invest in best practices and technologies, and those that cannot or will not. Those that can afford to invest in security are still targets, but they are *too expensive of targets* to be considered by most financially motivated cyber criminals. Trying to break into a well fortified company for weeks on end is an economically irrational use of resources when there are plenty of cheaper targets. These targets are well below the cyber security poverty line and can be compromised with minimal time, effort, and cost.

Coveware believes that every private security company has an obligation to provide services that make it easier for organizations to lift themselves above the cyber security poverty line. The higher the threshold (i.e. cost) to pull off an attack, the lower the profitability for the cyber crime industry. While marketing buzzwords like 'artificial intelligence' and 'machine learning,' along with the latest zero-day exploit used by an APT get headlines, the reality is that the majority of the damage to our economy and public organizations is NOT caused by highly sophisticated APTs or nation-state actors. Damage to these organizations is caused by financially motivated cyber criminals using repetitive and unremarkable, but highly profitable, means of attack.

Recognizing the most common and economically favorable vectors of ingress, and helping organizations close the same, should be our top priority. The implementation of highly effective solutions does not need to be complex or costly, but is actually very straightforward and inexpensive. We think all software companies should take the fundamentals of our recommendations as a responsibility.

## How to Reduce Exposure to Ransomware Attacks and Data Breaches

We suggest one simple initiative that will dramatically decrease the volume of attacks. This suggestion is rooted in our belief that in order to make substantive change, we must alter the economics of the cyber extortion industry. The industry's profitability MUST be altered,

otherwise it will continue to expand. While there are LOTS of ways to either increase costs, decrease revenue, or increase risk for cyber criminals, we must be pragmatic and work big-to-small. This does not mean other initiatives should be abandoned, it just means priority should be set based on the magnitude of the return on effort. We should do the things that have the greatest amount of impact using the least amount of resources in the shortest possible time.

**Recommendation #1: Eliminate RDP as an attack vector**

Since Coveware began collecting and reporting data (in Q3 of 2018), RDP has remained as the predominant attack vector. Compromised RDP credentials are used in 30-60% of ransomware attacks. This has not changed materially in 2 years. RDP is simply too cheap and reliable as a means to carry out an attack. Economically rational actors cannot ignore how profitable and predictable RDP based attacks are. There is no reason to use expensive 'zero-day' exploits or bespoke malware when less than $100 dollars allows a threat actor to gain access to a network. If compromised RDP credentials are eliminated or materially curtailed as an attack vector, the economic ripples to the cyber extortion industry will be material. First, the decrease in supply of credentials will lead to an increase in the price of whatever credentials remain available. A set of credentials that used to cost $50 may now cost $200. This will raise the barrier to entry as start up costs will increase, thereby decreasing the available labor pool of new criminals that can afford to participate. The decrease in supply of RDP credentials will put corresponding upward pressure on other means of attack, raising the cost as more actors that used to favor RDP are forced into higher cost activities. Since RDP attacks comprise roughly 50% of all attacks, the removal of these attacks would dramatically lower the average conversion rates, thereby lowering the expected proceeds of an attack. Additionally, swapping into alternative attack vectors would require more technical skills (along with capital). Removing non-technical actors from the available pool of participants would decrease the volume of attacks.

**How do we close RDP as an attack vector for everyone?**

The first step is recognizing how dangerous RDP is when misconfigured. A misconfigured RDP port is akin to globally advertising that you leave the front door of your home wide open. Threat actor specialists who run IP port scanning bots have emerged. These malicious programs scour every IP address on the internet, and can detect a new RDP port that is open misconfigured. A new RDP port will typically be discovered by one of these bots within 90 seconds of its first connection to the open internet (see Appendix F). The bot first locates the machine, and then immediately begins to brute force access. It will not stop until it is either locked out or has successfully guessed the user name and password.

Most organizations that misconfigure RDP do so out of convenience, with a misunderstanding of the risks. They assume they are too small to be a target, and don't bother to take the proper precautions. As we have described above, anyone that opens RDP to the internet is a target. There are currently close to 4.7 million misconfigured RDP machines open to the internet. The supply is massive, making the corresponding cost of compromise low. Until this is fixed, the

attacks will continue.

**Properly Configuring RDP**

We have provided a simple guide in Appendix G that outlines the proper steps to configure RDP. What is important to recognize is that applying proper RDP configuration DOES NOT require the purchase of expensive hardware or software. It only requires the awareness of this risk, and the time and effort to patch the issue. We offer it as the main recommendation of this testimony BECAUSE of its simplicity AND the relatively high impact it could have given the minimal investment necessary. The Committee has specifically requested what steps "resource-constrained enterprises and organizations (both public and private) can take to reduce their exposure." Coveware can offer no greater recommendation that has so substantial a return on investment given how common RDP based ransomware attacks are. The fix only requires awareness and time and effort to properly configure. The result could lead to a dramatic reduction in attacks, and corresponding decrease in the profitability of the cyber extortion industry. If we are able to eliminate or significantly curtail RDP as an attack vector, we will tip the industry's unit economics away from the criminals.

**RDP Case Study - Proof this will work**

In April of 2020 a well known cyber insurance company launched an initiative to reduce the number of RDP based ransomware attacks claimed by their policyholders. In order to do so they proactively scanned their policy holders for vulnerability, screened renewals and new applications for exposed RDP, and then provided remediation steps to the policy holders. They followed up with all their policyholders and even offered financial incentives, via lower policy premiums, to organizations that took their mitigation steps. In the 4 months that followed the launch of this initiative, their total volume of ransomware claims dropped by 65%. RDP was virtually eliminated as an attack vector for the claims they did receive. There is nothing special about this single insurance company's policy holders, they are the same size and shape our Nation's small businesses and public sector organizations. The same results are possible across a broader swath of exposed organizations.

**Recommendation #2: Require multi-factor authentication for Administrative Users.**

While we would prefer ALL users of a network be required to pass through multi-factor authentication, we are pragmatists and recognize that a lot of organizations simply won't deploy these requirements to their users. Our recommendation is that administrative systems like Active Directory, security applications, and back up systems require an administrator to authenticate with two factors. In the history of Coveware, spanning thousands of attacks on companies large and small, we have NEVER seen multi-factor authentication overcome by a threat actor.

# Conclusions

Threats to enterprises and organizations from the cyber extortion industry will never disappear, but the depth and impact of this criminal industry on our country is fully within our control. Applying an economic lens to the problem, and working big-to-small as we have suggested, will tip the industry into contraction. We will never be free of threats, but we must turn the tides of this criminal industry and minimize the impact it has on our country. When combined with new security policy and a healthy dose of law enforcement, we see a very different future that is both practical and achievable. It would not take years to correct, and most importantly, it does not require a massive increase in spending. All it takes is awareness, understanding, and willpower.

Thank you for your time.

~Bill Siegel
CEO and Co-Founder of Coveware

# Appendices

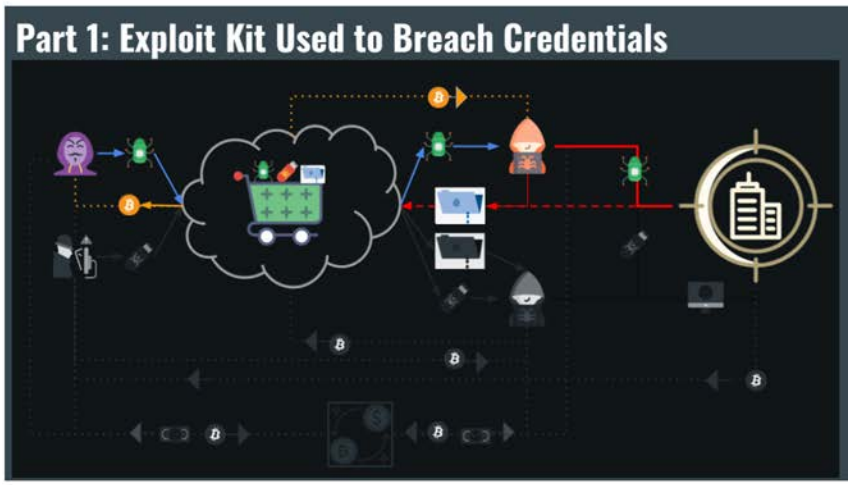
**Appendix A**

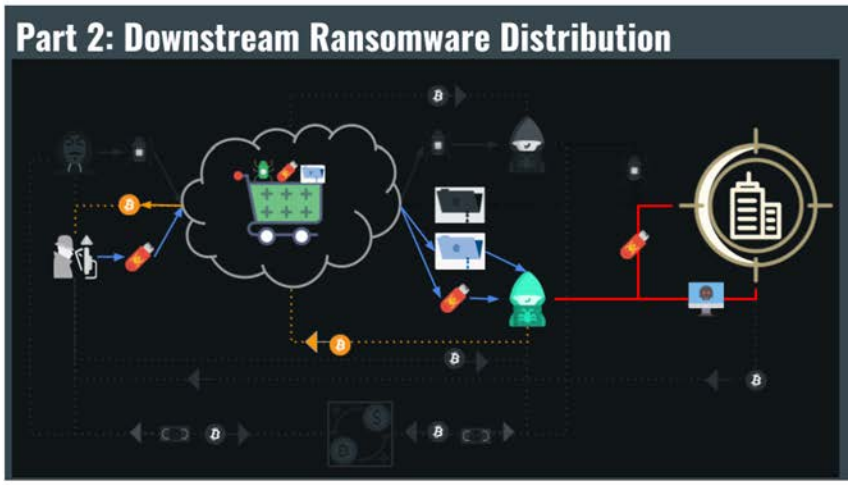
Common Ransomware groups by market share of attacks

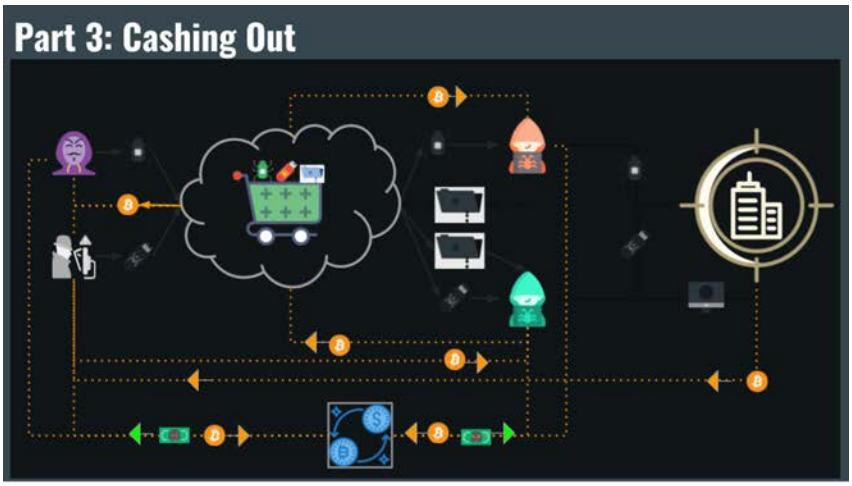
| Rank | Ransomware Type | Market Share % | Change in Ranking from Q1 2020 |
|---|---|---|---|
| 1 | Sodinokibi | 15.4% | - |
| 2 | Maze | 7.7% | +7 |
| 2 | Phobos | 7.7% | +1 |
| 4 | Netwalker | 7.1% | +6 |
| 5 | Dharma | 6.4% | -2 |
| 6 | Ryuk | 5.1% | -4 |
| 7 | Mamba | 4.5% | -2 |
| 8 | Snatch | 4.2% | -1 |
| 9 | Lockbit | 4.2% | +4 |
| 10 | DeathHiddenTear | 3.9% | +4 |

**Appendix B**

Flow chart of a typical ransomware attack showing different industry groups, specialists, and coordination.



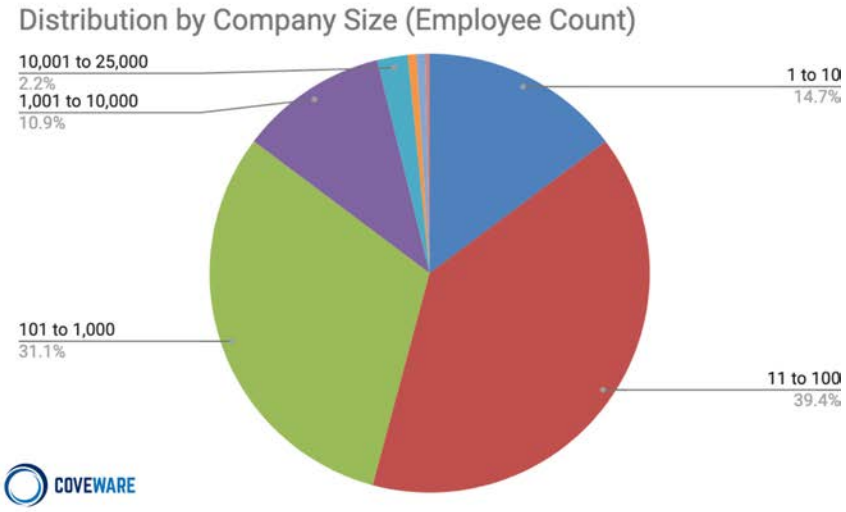

Part 3: Cashing Out

**Appendix C**

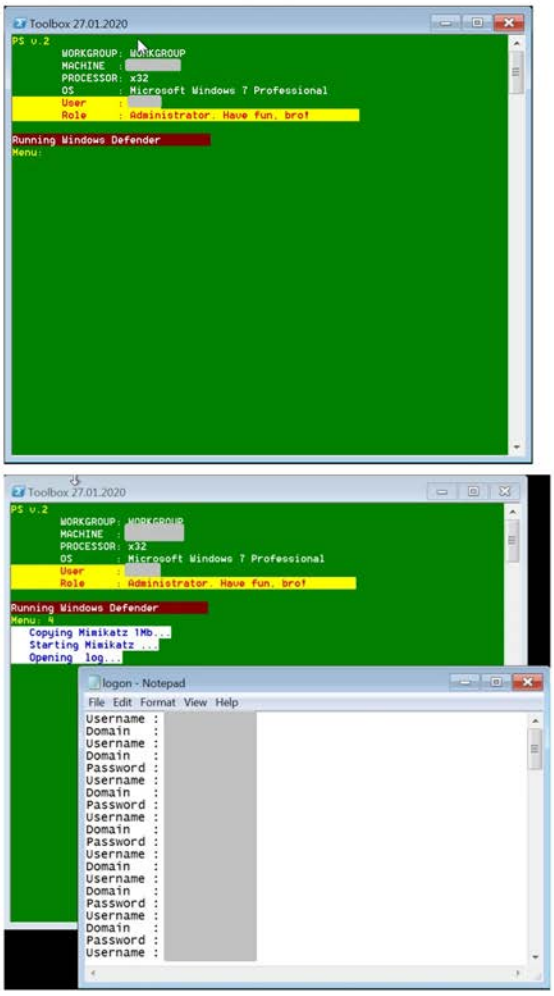
Increasing size of average ransom payments

COVEWARE

**Appendix D:**
Average size of a company impacted by ransomware in Q2 2020.



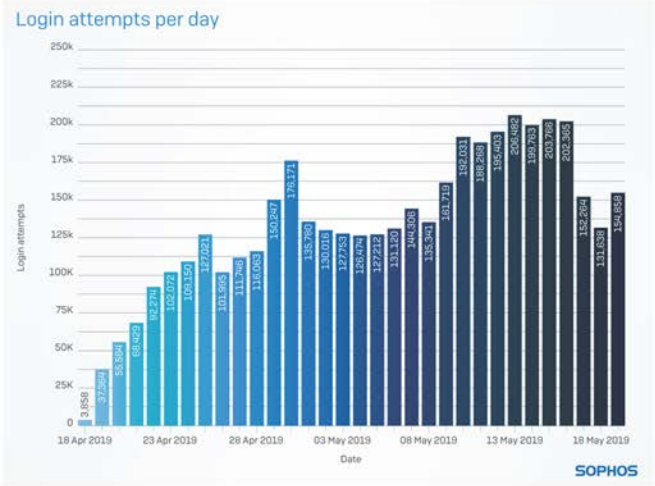
**Appendix E:**
Examples of simple to use, Ransomware-as-a-Service kits




(Source: Sophos & BleepingComputer)

**Appendix F:**

Login attempts over a 30 day period on a standard, improperly secured RDP machine




(Source: Sophos)

**Appendix G:**

Common steps to properly secure RDP:

1. Proactively apply OS and software patches: Keep OS and RDP related software up to date. Don't wait for something to break.
2. Strong Passwords and MFA: RDP connections should require strong passwords and multi-factor authentication (either at VPN or RDP level).
3. Limit Access or White List IP Address: Access granted only via a VPN session or only to a select whitelist of IP ranges.
4. Lockout: Access should be blocked after a short number of login attempts fail to prevent brute forcing.
5. The default port number should be changed from default (3389) to a random port number.
6. No exceptions. If a manager or noisy user constantly complains about tedious RDP security protocols then their RDP privileges should be put on warning.

**Post-Hearing Questions for the Record**
**Submitted to Brandon Wales**
**From Ranking Member Maggie Hassan**

**Subcommittee on Federal Spending Oversight and Emergency Management**
**"State and Local Cybersecurity: Defending our Communities from Cyber Threats amid COVID-19"**

**December 2, 2020**

***** Due to the change-over in Administration, responses were not received to these questions for the record. *****

1. We have recently heard some concerns about the status and funding of the Continuous Diagnostics and Mitigation (CDM) program in CISA. Can you give us an update on the status of the program and how the future of the program looks, including any funding concerns?

2. You mentioned during the hearing that CISA has been helping FEMA review the portions of Homeland Security Grant proposals that deal with cybersecurity.

    a. With that experience in mind, how involved do you believe CISA should be in a federal cybersecurity grant program for state and local governments, should Congress create such a program? Does CISA have the capability to effectively manage a grant program?

    b. Is CISA offering guidance to states on what type of investments to prioritize in their grant proposals? If so, are states using that guidance?

    c. What does CISA believe should be included in any cybersecurity grant proposal? What would give CISA confidence that the grant money would be going towards the most important necessary investments?

3. You mentioned during the hearing that, similar to what CISA has done with election infrastructure and election security, you want to see CISA build "a national community with school districts" to support them on cybersecurity. Also similar to election infrastructure, school districts are a part of a critical infrastructure subsector: the Education Facilities subsector of the Government Facilities sector. Can you further flesh out what you mean by "building a national community with school districts?" What lessons learned from the work done with the Election Infrastructure subsector does CISA intend to apply in support of the Education Facilities subsector? What is CISA doing to support the Education Facilities subsector?

4. You mentioned during the hearing that CISA is encouraging school districts to join the Multi-State Information Sharing and Analysis Center (MS-ISAC). Do you think schools would benefit from establishing their own dedicated ISAC?

**Post-Hearing Questions for the Record**
**Submitted to Denis Goulet**
**From Ranking Member Maggie Hassan**

**Subcommittee on Federal Spending Oversight and Emergency Management**
**"State and Local Cybersecurity: Defending our Communities from Cyber Threats amid COVID-19"**

**December 2, 2020**

1. North Dakota has been working on developing a shared security operations center with other states where states will be able to share both information and operational resources, including pooling resources in response to cybersecurity incidents.[1] Do you believe states should be working together operationally and not just sharing information, similar to the shared security operations center being developed and led by North Dakota? What do you see as the benefits and drawbacks of this approach?

NASCIO has been longtime advocates of a whole-of-state approach to cybersecurity – which as I discussed in my testimony, focuses on centralized governance, operations and information sharing among stakeholders who have clearly defined roles to play when a cyber incident occurs. While I believe that increased collaboration and information sharing among states should be a long-term goal, we frankly are not there yet from a national perspective. My current focus in New Hampshire is improving upon and maturing relationships within the state – from working to improve the cybersecurity posture of local and municipal governments, other state agencies and with our school districts. Centralizing cybersecurity and implementing a whole-of-state approach are nearly universal goals of every state CIO across the country. While the current efforts in North Dakota are laudable, the truth is most states lack organizational and operational models, as well as adequate funding, within their own borders.

While the establishment of interstate or regional security operations centers may prove to be a challenging endeavor for the majority of states, there are currently existing models that states may be able to leverage to further information sharing. All states, as well as thousands of local governments, are members of the Multi-State Information Sharing and Analysis Center (MS-ISAC). NASCIO has long been a strong advocate for the MS-ISAC, which has a consolidated security function as evidenced by its recent pilot program with the expanded deployment of Albert sensors. Both the MS-ISAC and the Department of the Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) provide state and local governments with timely and vitally important threat information sharing.

There are a couple of potential issues I can foresee concerning the creation of interstate security operations centers. The first being concerns among state legislatures and governors offices who may not want sensitive information shared across state lines. There is also the potential for funding issues as states are already grappling with revenue shortfalls from the ongoing

[1] https://statescoop.com/north-dakotas-building-a-cybersecurity-operations-center-and-everyones-invited/

pandemic. While these issues could certainly be overcome, it is important for states to consider these policy and funding implications.

If Congress does want to encourage states to adopt the model of shared security operations centers, I think it would be necessary to develop a playbook or guidebook of best practices. NASCIO has done a tremendous job of producing dozens of research papers and guidebooks over the years on the most important issues facing state CIOs, but I am not aware of any organization or association that has conducted in-depth research on this particular topic.

○