EXAMINING DHS'S CYBERSECURITY MISSION

HEARING

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY AND INFRASTRUCTURE PROTECTION

OF THE

COMMITTEE ON HOMELAND SECURITY
HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTEENTH CONGRESS

FIRST SESSION

OCTOBER 3, 2017

Serial No. 115–30

Printed for the use of the Committee on Homeland Security

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

U.S. GOVERNMENT PUBLISHING OFFICE
28–419 PDF WASHINGTON : 2018

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY

Michael T. McCaul, Texas, *Chairman*

Lamar Smith, Texas
Peter T. King, New York
Mike Rogers, Alabama
Jeff Duncan, South Carolina
Lou Barletta, Pennsylvania
Scott Perry, Pennsylvania
John Katko, New York
Will Hurd, Texas
Martha McSally, Arizona
John Ratcliffe, Texas
Daniel M. Donovan, Jr., New York
Mike Gallagher, Wisconsin
Clay Higgins, Louisiana
John H. Rutherford, Florida
Thomas A. Garrett, Jr., Virginia
Brian K. Fitzpatrick, Pennsylvania
Ron Estes, Kansas

Bennie G. Thompson, Mississippi
Sheila Jackson Lee, Texas
James R. Langevin, Rhode Island
Cedric L. Richmond, Louisiana
William R. Keating, Massachusetts
Donald M. Payne, Jr., New Jersey
Filemon Vela, Texas
Bonnie Watson Coleman, New Jersey
Kathleen M. Rice, New York
J. Luis Correa, California
Val Butler Demings, Florida
Nanette Diaz Barragán, California

Brendan P. Shields, *Staff Director*
Steven S. Giaier, *Deputy Chief Counsel*
Michael S. Twinchek, *Chief Clerk*
Hope Goins, *Minority Staff Director*

SUBCOMMITTEE ON CYBERSECURITY AND INFRASTRUCTURE PROTECTION

John Ratcliffe, Texas, *Chairman*

John Katko, New York
Daniel M. Donovan, Jr., New York
Mike Gallagher, Wisconsin
Thomas A. Garrett, Jr., Virginia
Brian K. Fitzpatrick, Pennsylvania
Michael T. McCaul, Texas *(ex officio)*

Cedric L. Richmond, Louisiana
Sheila Jackson Lee, Texas
James R. Langevin, Rhode Island
Val Butler Demings, Florida
Bennie G. Thompson, Mississippi *(ex officio)*

Kristen M. Duncan, *Subcommittee Staff Director*

CONTENTS

Page

STATEMENTS

WITNESSES

APPENDIX

EXAMINING DHS'S CYBERSECURITY MISSION

Tuesday, October 3, 2017

U.S. House of Representatives,
Committee on Homeland Security,
Subcommittee on Cybersecurity and
Infrastructure Protection,
Washington, DC.

The subcommittee met, pursuant to notice, at 10:04 a.m., in room HVC–210, Capitol Visitor Center, Hon. John Ratcliffe (Chairman of the subcommittee) presiding.

Present: Representatives Ratcliffe, McCaul, Garrett, Fitzpatrick, Donovan, Katko, Richmond, Thompson, Demings, and Langevin.

Mr. Ratcliffe. The Committee on Homeland Security's Subcommittee on Cybersecurity and Infrastructure Protection will come to order. First of all, I am sure I speak for all of us here on the dais in expressing our deepest condolences to all of the family members and all of the victims of yesterday's tragedy in Las Vegas.

Events like the one yesterday really demand the utmost humanity in response to such blind hate and evil, and hopefully it will give us all a renewed sense of purpose today as we approach the tasks of the day.

The subcommittee is meeting today to receive testimony regarding the Department of Homeland Security's cybersecurity mission. I recognize myself for an opening statement.

We are here today at the start of National Cybersecurity Awareness Month to discuss what I believe is one of the defining public policy challenges of this generation, the cybersecurity posture of the United States.

We have seen cyber attacks hit practically every sector of our economy, with devastating impacts to both Government agencies and the private sector alike. It is our shared duty to ensure that we are doing our very best to defend against the very real threat our cyber adversaries are posing.

But make no mistake. The cybersecurity challenges we face are about much, much more than simply protecting bottom lines or intellectual property or even our Nation's most Classified information. They also impact the personal and often irreplaceable information of every American.

This year we have seen on a grand scale just how much damage can be done by a single individual or entity looking to conduct a cyber attack. The Equifax breach shows that it takes only one bad actor and only one exploitable vulnerability to do something to compromise the information of 145 million Americans. This is not the first cyber attack that has garnered National attentions, and unfortunately it almost assuredly will not be the last.

As the members of this panel and as our witnesses here today know well, there is no silver bullet or guaranteed technology to fix the cybersecurity problem. Rather, we need to be part of an ongoing, sustained, dedicated, persistent, and comprehensive campaign to ensure the United States remains the world's cybersecurity superpower.

We will continue to need a sharp work force, collective efforts in public-private partnerships and the leadership of our Government agencies to leverage our resources and to counter our highly sophisticated cyber adversaries.

Today, the subcommittee meets to hear from the Government officials that are charged with meeting these cyber threats. These are the folks on the front lines day in and day out.

DHS is the Federal Government's lead civilian agency for cybersecurity, and within it, the National Protection and Programs Directorate, or NPPD, leads our National effort to safeguard and enhance the resilience of our Nation's physical and cyber infrastructure, helping Federal agencies and, when requested, the private sector harden their networks and respond to cybersecurity incidents.

NPPD partners with critical infrastructure owners and operators and other homeland security enterprise stakeholders to offer a wide variety of cybersecurity capabilities, such as system assessments, incident response and mitigation support, and the ability to hunt for malicious cyber activity.

This collaborative approach to mitigating cyber incidents is meant to prioritize meeting the needs of DHS's partners, and is consistent with the growing recognition among Government, academic, and corporate leaders, that cybersecurity is increasingly interdependent across sectors and must be a core aspect of all risk management strategies.

This committee has been working hard to ensure that NPPD and DHS in its entirety has the necessary authorizations and organization it needs to combat growing cyber threats. DHS needs a strong and sharp work force and an efficient organizational structure to support both its cybersecurity and its infrastructure protection missions.

Earlier this year, the committee marked up and passed H.R. 3359, the Cybersecurity and Infrastructure Security Agency Act of 2017, to reorganize and to strengthen NPPD.

As the cyber threat landscape continues to evolve, so should DHS. In doing so, H.R. 3359 is the tool that we will use to bring NPPD to a more visible role in the cybersecurity of this Nation.

As a committee and as a Congress, we have taken important steps in the right direction with legislation on information sharing, on modernizing the Federal Government's information technology, and in getting our State and local officials the cybersecurity support that they need.

Some of these programs have been years in the making. Real-time collaboration between the Government and the private sector is a lofty and worthwhile goal. Through the automated indicator-sharing program, or AIS, DHS has been partnering with industry to create and enhance that broader information-sharing environment, and we have made progress in the right direction.

While we know that proactive information sharing is only as good as the information being provided, that type of relationship can only be made possible with a strong foundation of trust.

I am looking forward to a robust discussion today, not only about how the Department can be best organized and equipped to ensure that we are leveraging the resources of the Federal Government toward this immense challenge, but also how the Government can forge and grow the necessary partnerships to achieve the greater cybersecurity for our Nation.

We have to get this right, because new technologies, the internet of things, driverless cars, artificial intelligence, and quantum computing are all rapidly evolving. So we need to be securing at the speed of innovation and not at the speed of bureaucracy. We are in an era that requires flexibility, resiliency, and discipline, and I hope that I will hear those values operationalized in the forthcoming testimony.

Cyber space plays an increasingly dominant role in the fabric of the American society, and it will take continued collaboration across the public, private, international, and domestic spaces, to keep making the advancements needed to prioritize cybersecurity for our country.

I know this is a responsibility that everyone on this subcommittee takes extraordinarily seriously, and I look forward to the discussion today with our witnesses.

[The prepared statement of Chairman Ratcliffe follows:]

Statement of Chairman John Ratcliffe

October 3, 2017

We are here to today, at the start of National Cybersecurity Awareness Month, to discuss what I believe is one of the defining public policy challenges of our generation—the cybersecurity posture of the United States. We have seen cyber attacks hit practically every sector of our economy with devastating impacts to both Government agencies and the private sector alike—and it's our shared duty to ensure we're doing our best to defend against the very real threat our cyber adversaries pose.

But make no mistake—the cybersecurity challenges we face are about much, much more than simply protecting bottom lines, or intellectual property, or even our Nation's most Classified information. They also impact the personal, often irreplaceable information, of every American.

This year, we've seen—on a grand scale—just how much damage can be done by a single individual or entity looking to conduct a cyber attack. It may take only one bad actor and only one exploitable vulnerability to do something such as compromise the information of 143 million Americans.

This is not the first cyber attack that's garnered National headlines, and unfortunately—it almost assuredly will not be the last.

As the members of this panel and as our witnesses here today know well, there is no silver bullet or guaranteed technology to "fix" the cybersecurity problem. Rather, this is part of an on-going, sustained, and comprehensive campaign to ensure the United States remains the world's cybersecurity superpower.

We will continue to need a sharp workforce, the collective efforts in public-private partnerships, and the leadership of our Government agencies to leverage our resources and counter our highly sophisticated cyber adversaries.

Today, this subcommittee meets to hear from the Government officials charged with meeting these cyber threats. These are the folks on the front lines day in and day out.

DHS is the Federal Government's lead civilian agency for cybersecurity, and within it, the National Protection and Programs Directorate, or NPPD, leads our National effort to safeguard and enhance the resilience of the Nation's physical and cyber infrastructure, helping Federal agencies and, when requested, the private sector harden their networks and respond to cybersecurity incidents.

NPPD partners with critical infrastructure owners and operators and other homeland security enterprise stakeholders to offer a wide variety of cybersecurity capabilities, such as system assessments, incident response and mitigation support, and the ability to hunt for malicious cyber activity.

This collaborative approach to mitigating cyber incidents is meant to prioritize meeting the needs of DHS partners, and is consistent with the growing recognition among Government, academic, and corporate leaders that cybersecurity is increasingly interdependent across sectors and must be a core aspect of risk management strategies.

This committee has been working hard to ensure that NPPD—and DHS in its entirety—has the necessary authorizations and organization it needs to combat growing cyber threats.

DHS needs a robust workforce and an efficient organizational structure to support both its cybersecurity and infrastructure protection missions.

Earlier this year, this committee marked up and passed H.R. 3359—the Cybersecurity and Infrastructure Security Agency Act of 2017 to reorganize and strengthen NPPD.

As the cyber threat landscape continues to evolve, so should DHS, and in doing that, H.R. 3359 is the tool we'll use to bring "NPPD" to a more visible role in the cybersecurity of this Nation.

As a committee, and as a Congress, we have taken important steps in the right direction with legislation on information sharing, modernizing the Federal Government's information technology, and in getting our State and local officials the cybersecurity support they need.

Some of these programs have been years in the making.

Real-time collaboration between the Government and the private sector is a lofty and worthwhile goal. Through the Automated Indicator Sharing program, or AIS, DHS has been partnering with industry to create and enhance that broader information-sharing environment—and we've made progress in the right direction.

While we know that proactive information sharing is only as good as the information being provided, that type of relationship can only be made possible with a strong foundation of trust.

I'm looking forward to a robust discussion today, not only about how the Department can be best organized and equipped to ensure that we are leveraging the resources of the Federal Government toward this immense challenge, but also how the Government can forge and grow the necessary partnerships to achieve greater cybersecurity for our Nation.

We have to get this right because new technologies—the internet of things, driverless cars, artificial intelligence, and quantum computing—are rapidly evolving.

We need to be securing at the speed of innovation—not of bureaucracy.

Because we are in an era that requires flexibility, resiliency, and discipline and I hope I will hear those values operationalized in the forthcoming testimony.

Cyber space plays an increasingly dominant role in the fabric of our society, and it will take continual collaboration across the public, private, international, and domestic spaces to keep making the advancements needed to prioritize cybersecurity for our country.

I know this is a responsibility that everyone on this subcommittee takes extraordinarily seriously, and I look forward to the discussion today with our witnesses.

Mr. RATCLIFFE. The Chair now recognizes the Ranking Minority Member of the subcommittee, the gentleman from Louisiana, Mr. Richmond, for his opening statement.

Mr. RICHMOND. Thank you, Mr. Chairman.

Good morning. I am pleased that we are kicking off Cybersecurity Awareness Month by talking to the Department of Homeland Security about its cybersecurity mission and how Congress can help ensure DHS is well-positioned to protect critical infrastructure from cyber attacks.

Before I begin, however, I would like to send my condolences to the families of the victims of Sunday night's horrific shooting. To the survivors, you are in our thoughts and prayers. To the brave first responders who ran into danger when everyone else was running away from it, we are grateful.

The Democrats on this committee have said this before, but it bears repeating. At some point, we are gonna have to come together and enact sensible gun legislation. As the Congressman representing New Orleans, I cannot sit silently as the President insults the hurricane survivors of Puerto Rico and the San Juan mayor who is trying to help them.

I have been through Katrina, and I know what it is like when you are at your most vulnerable moment and you have lost everything. What you are looking for is assistance because it is beyond your capacity to respond to a storm of that magnitude.

So having seen the people grieve the loss of their homes and businesses and struggle to piece their lives back together, I can tell you that the last thing the people in Puerto Rico and the Virgin Islands need are insults. I urge the President to take a break from Twitter, roll up his sleeves and get to work.

Turning to the issue at hand, as I mentioned, I represent New Orleans, which has significant energy sector assets. Last month, we heard disturbing reports of a new wave of efforts to breach energy sector networks in the United States.

According to Symantec, in some cases, hackers achieved unprecedented access to operational systems. In light of these reports, I am interested to know how the Department of Homeland Security and the Department of Energy are working together to secure energy sector networks and make them more resilient.

Additionally, as a Member of this committee and the Congressional Task Force on Election Security, I am eager to hear about DHS's activities to secure our election systems.

Although the administration's commitment to the critical infrastructure designation appeared to waver earlier this year, I was encouraged when acting Secretary Duke told committee Democrats last month that there are no plans to rescind the designation.

With that comment, I look forward to hearing about the progress DHS is making to help State and local governments secure election infrastructure and whether the Department has adequate resources to carry out its responsibilities in that space.

For example, I understand there is a 9-month wait for a risk and vulnerability assessment and that some Secretaries of State have complained about the lengthy clearance process for election officials. I am concerned that these kinds of challenges may deter some States, particularly those hostile to the critical infrastructure designation, from taking full advantage of the resources DHS can bring to bear.

To that point, DHS has struggled to build some of the relationships necessary to executing its election security mission. Although I have heard that DHS is making progress in this regard, I am concerned mistakes made notifying certain Secretaries of State that their election infrastructure had been targeted, though it had not been, may have undermined the trust that DHS has sought to build.

I would be interested in learning, what do you need from Congress to address election infrastructure requests more quickly and build trust with the election infrastructure community?

Finally, when Ms. Manfra testified before the subcommittee in March, I asked when I could expect the DHS cybersecurity strategy. The strategy required pursuant to legislation I authored was due March 23. It still has not been submitted to Congress.

I understand the Trump administration did not fill leadership positions relevant to the execution of DHS cybersecurity strategy with any real sense of urgency and on-going vacancies may be contributing to the delays. But the strategy is 6 months overdue, and that is not acceptable.

With that, Mr. Chairman, I yield back the balance of my time.

[The prepared statement of Ranking Member Richmond follows:]

STATEMENT OF RANKING MEMBER CEDRIC L. RICHMOND

OCTOBER 3, 2017

I am pleased that we are kicking off cybersecurity awareness month by talking to the Department of Homeland Security about its cybersecurity mission and how Congress can help ensure DHS is well-positioned to protect critical infrastructure from cyber attacks.

Before I begin, however, I would like to send my condolences to the families of the victims of Sunday night's horrific shooting in Las Vegas. To the survivors, you are in our thoughts. To the brave first responders who ran into danger when everyone else was running away from it, we are grateful.

The Democrats on this committee have said this before, but it bears repeating: At some point, the Majority is going to have to stand up to the gun lobby and enact responsible gun control legislation.

And, as the Congressman representing New Orleans, I cannot sit silently as the President insults the hurricane survivors of Puerto Rico and the San Juan Mayor who is trying to help them.

Having seen people grieve the loss of their homes and businesses and struggle to piece their lives back together, I can tell you the last thing the people of Puerto Rico need are insults from the President. I urge the President to take a break from Twitter, roll up his sleeves, and get to work.

Turning to the issue at hand, as I mentioned, I represent New Orleans, which has significant energy sector assets. Last month, we heard disturbing reports of a "new wave" of efforts to breach energy sector networks in the United States. According to Symantec, in some cases, hackers achieved unprecedented access to operational systems.

In light of these reports, I am interested to know how the Department of Homeland Security and the Department of Energy are working together to secure energy sector networks and make them resilient.

Additionally, as a Member of this committee and of the Congressional Task Force on Election Security, I am eager to hear about DHS's activities to secure our election systems.

Although the administration's commitment to the critical infrastructure designation appeared to waver earlier this year, I was encouraged when Acting Secretary Duke told committee Democrats last month that "[t]here are no plans" to rescind the designation.

With that commitment, I look forward to hearing about the progress DHS is making to help State and local governments secure election infrastructure and whether the Department has adequate resources to carry out its responsibilities in that space.

For example, I understand there is a 9-month wait for a Risk and Vulnerability Assessment and that some Secretaries of State have complained about the lengthy clearance process for election officials. I am concerned that these kinds of challenges may deter some States—particularly those hostile to the critical infrastructure designation—from taking full advantage of the resources DHS can bring to bear.

To that point, DHS has struggled to build some of the relationships necessary to executing its election security mission. Although I have heard that DHS is making process in this regard, I am concerned mistakes made notifying certain Secretaries of State that their election infrastructure had been targeted——though it had not been—may have undermined the trust DHS has sought to build.

I will be interested in learning what do you need from Congress to address election infrastructure requests more quickly and build trust within the election infrastructure community.

Finally, when Ms. Manfra testified before the subcommittee in March, I asked when I could expect the DHS Cybersecurity Strategy. The strategy, required pursuant to legislation I authored, was due March 23. It still has not been submitted to Congress.

I understand the Trump administration did not fill leadership positions relevant to the execution of a DHS Cybersecurity Strategy with any real sense of urgency, and on-going vacancies may be contributing to the delays. But the strategy is 6 months overdue, and that is not acceptable.

Mr. RATCLIFFE. I thank the gentleman.

The Chair now welcomes and recognizes the Chairman of the full committee, my colleague from Texas, Mr. McCaul, for any opening statement that he might have.

Chairman MCCAUL. Thank you, Chairman Ratcliffe.

I also would like to extend my thoughts and prayers to the victims and family members of the horrifying tragedy in Las Vegas. I am hopeful that as Americans we can come together and prevent such violence from happening in the future.

I am pleased to be here at this important hearing today, with our distinguished guests here at this hearing. America's National security is threatened by Islamist terrorists, tyrannical regimes building and proliferating weapons of mass destruction, human traffickers, and transnational gang members like MS–13 who stream across our border.

These threats are well-known, and we need to do everything we can to stop them as we see them coming. However, we also find ourselves in the crosshairs of invisible attacks and sustained cyber war from nation-states and other hackers.

As we become more and more reliant on computers and smartphones in both our personal and professional lives, everyone is a potential target. Sadly, many of us have already been victims.

Over the past few years, we have seen many successful large-scale cyber attacks take place. In early September, hackers were able to breach Equifax, a credit reporting agency, gaining access to sensitive information on as many as 143 million people.

In 2016, we know that Russia tried to undermine our electoral system and democratic process, and in 2015, we learned that China stole over 20 million security clearances, including mine, and probably some here at this dais. These kinds of violations are simply unacceptable.

I am proud to say that over the last few years this committee, the Committee on Homeland Security, has recognized these threats and has led the charge in the Congress to strengthen the defense of our Nation's networks.

In 2014, we enacted several important bills and empowered DHS to bolster its work force, codified DHS's cyber center, and updated FISMA for the first time in 12 years. A year later, the Cybersecurity Act became law, which enhances information sharing and makes DHS the lead conduit for cyber threat indicators and defensive measures within the Federal Government.

While information sharing has come a long way, the WannaCry ransomware attack recently illustrated just how important and beneficial these relationships are. Just last week, Rob Joyce, the cybersecurity coordinator at the White House, noted that we needed to find a way to provide the private sector with more expansive access to cyber threat information in a controlled setting, something I believe we need to strengthen.

Moreover, issues relating to the sharing of Classified information with the private sector, like accrediting SCIF space, granting security clearances to key personnel and enabling consistent two-way communications are issues we are looking at closely.

In other words, we have made great progress in the way indicators are shared. But I want to examine if we can do more regarding the overall sharing of Classified information.

Earlier this year, I was pleased to see President Trump issue an Executive Order to strengthen the cybersecurity of Federal networks and critical infrastructure. Going forward, I am hopeful that the House can advance legislation that I have introduced to elevate NPPD as a stand-alone agency and better support the cybersecurity mission at DHS.

This month is National Cybersecurity Awareness Month, a time to learn more about these threats and offer ideas on how we can best secure ourselves against these growing threats. While we have had some success on this issue, we must do more.

Our cyber enemies, including terrorists, are always evolving, looking for new ways to carry out their next attack. Fortunately, this is an issue that I believe transcends party lines. It is not a Republican or Democrat issue. So let's work together to make our cybersecurity strong and keep the American people safe.

Again, I would like to thank the witnesses for being here today, and thank you for your service. A very important component of the Department that often, as I mentioned in my opening, we focus a lot on counterterrorism and the border among other things. But I consider this mission that the Department has to be one of the most important that this Nation faces.

So I look forward to the conversation on how Congress and the Executive branch can work together, and how we can work with leaders in the private sector to enhance the Nation's cybersecurity. So, with that I would like to yield back to the Chairman, and if I may, submit my questions for the record.

[The statement of Chairman McCaul follows:]

STATEMENT OF CHAIRMAN MICHAEL T. MCCAUL

OCTOBER 3, 2017

Thank you, Chairman Ratcliffe. I would also like to extend my thoughts and prayers to the victims and family members of the horrifying tragedy in Las Vegas. I am hopeful that as Americans, we can come together and prevent such violence from happening again.

America's National security is continually threatened by Islamist terrorists, tyrannical regimes building and proliferating weapons of mass destruction, and human traffickers and transnational gang members like MS–13 who stream across our border. These threats are well-known, and we need do everything we can to stop them as we see them coming.

However, we also find ourselves in the crosshairs of invisible attacks in a sustained cyber war from nation-states and other hackers. As we become more and more reliant on computers and smartphones in both our personal and professional lives, everyone is a potential target and sadly, many of us have already been victims.

Over the past few years we have seen many successful large-scale cyber attacks take place. In early September, hackers were able to breach Equifax, a credit reporting agency, gaining access to sensitive information on as many as 143 million people.

In 2016, we know that Russia tried to undermine our electoral system and democratic process and in 2015, we learned that China stole over 20 million security clearances including mine. These kinds of violations are simply unacceptable.

I am proud to say that over the last few years, the Committee on Homeland Security has recognized these threats and led the charge to strengthen the defense of our Nation's networks.

In 2014, we enacted several important bills that empowered DHS to bolster its work force, codified DHS's cyber center, and updated FISMA for the first time in 12 years. A year later, the Cybersecurity Act became law, which enhances information sharing and makes DHS the lead conduit for cyber threat indicators and defensive measures within the Federal Government.

While information sharing has come a long way, the WannaCry ransomware attack recently illustrated just how important and beneficial those relationships are.

Just last week Rob Joyce, the cybersecurity coordinator at the White House, noted that we need to find a way to provide the private sector with more expansive access to cyber threat information in a controlled setting; something I believe we need to strengthen.

Moreover, issues relating to the sharing of Classified information with the private sector, like accrediting SCIF space, granting security clearances to key personnel, and enabling consistent two-way communication, are issues we are looking at closely.

In other words, we have made progress in the way indicators are shared but I want to examine if we can do more regarding the overall sharing of Classified information.

Earlier this year, I was pleased to see President Trump issue an Executive Order to strengthen the cybersecurity of Federal networks and critical infrastructure. Going forward, I am hopeful that the House can advance legislation that I have introduced to elevate NPPD as a stand-alone agency and better support the cybersecurity mission at DHS.

This month is National Cybersecurity Awareness Month, a time to learn more about these threats and offer ideas on how we can best secure ourselves against these growing threats. While we have had some success on this issue, we must do more.

Our cyber enemies, including terrorists, are always evolving, looking for new ways to carry out their next attack. Fortunately, this is an issue that transcends party lines. Let's work together to make our cybersecurity strong and keep the American people safe.

I would like to thank today's witnesses for their time and their service. I look forward to our conversation about how Congress and the Executive branch can work together and also with leaders in the private sector to enhance our Nation's cybersecurity.

I would also like to work with you, Chairman Ratcliffe, and our witnesses to bring our Members to the NCCIC before the end of the year to see the progress first-hand.

Thank you.

Mr. RATCLIFFE. I thank the Chairman.

The Chair now welcomes and recognizes the Ranking Minority Member of the full committee, the gentleman from Mississippi, Mr. Thompson, for his opening statement.

Mr. THOMPSON. Thank you very much. Good morning. I would like to thank Chairman Ratcliffe and Ranking Member Richmond for holding today's hearing to examine the work DHS is doing to shore-up our Nation's cyber defenses.

There is no doubt that our country is facing an ever-evolving rate of cyber threats. As we stand here today, our enemies are thinking of new and novel ways to strike at everything from banks to hospitals and chemical facilities. Nefarious actors even want to disrupt some of our most basic institutions.

Last year, we learned that our Nation's election system served as a new frontier for cyber attacks. With every passing day, we learn of new ways cyber operatives are looking to exploit everything from the media we consume to the databases that store voter registration data.

In this country, there is nothing more sacred than the ability to engage in civic activity, and cyber criminals are seeking to undermine our democracy. Furthermore, as I watch the devastation unfold in Texas, Florida, Puerto Rico, and the Virgin Islands, I am reminded of the fragility of our systems.

Disrupting the systems we rely on for power, fuel, food, and water, can be deadly, regardless of whether it is caused by a cyber attack or a natural disaster. In short, the digital networks we rely on for our day-to-day life are facing a multitude of threats. To respond to these treats, Congress has put its trust in DHS.

Over the past few years, Congress, by way of this committee, has consistently expanded DHS's cybersecurity mission, giving the Department a key role in securing Federal networks, as well as the systems that support our Nation's critical infrastructure.

The Department made huge strides in implementing these new authorities, including by standing up an automated system to share cyber threat data and advising the new election infrastructure subsector on how to promote cyber hygiene with election administrators throughout the country. We cannot, however, expect DHS to carry out these responsibilities with both hands tied behind its back.

To be successful, the Department needs adequate resources, a robust staff, strong leadership and a clear strategy. Unfortunately, this administration has been gravely unfocused when it comes to cybersecurity.

President Trump falsely promised to deliver a comprehensive plan to protect America's vital infrastructure from cyber attacks on the first day in office. It took months for the President to get around to issuing an Executive Order on cybersecurity.

Also a quarter of the 28-person National Infrastructure Advisory Council resigned in protest to President Trump's insufficient attention to cyber threats. President Trump floated the idea of an impenetrable cyber unit with Russia. At the same time, members of his administration were considering and ultimately deciding to ban the use of the Kaspersky products on Federal networks.

Within DHS, the chief information officer resigned after serving only 4 months. The National Programs and Protection Directorate, the Department's main cyber arm is still operating without a permanent under secretary.

Whether the men and women in this room are willing to acknowledge in an open setting, that they are struggling without this leadership, we can be certain that these gaps are making their job harder. I look forward to hearing from the panel today about how the Department is carrying out its cyber mission.

I hope that you will be candid with us about the obstacles you face. If there are areas where you need additional resources or legislative clarity, tell us how we can help. I am especially eager to hear from Ms. Hoffman about how DHS works with one of its key partners in securing critical infrastructure, the Department of Energy.

With that Mr. Chairman, I yield back.

[The statement of Ranking Member Thompson follows:]

STATEMENT OF RANKING MEMBER BENNIE G. THOMPSON

OCTOBER 3, 2017

There is no doubt that our country is facing an evolving array of cyber threats. As we stand here today, our enemies are thinking of new and novel ways to strike at everything from banks to hospitals and chemical facilities. Nefarious actors even want to disrupt some of our most basic institutions.

Last year, we learned that our Nation's election system served as a "new frontier" for cyber attacks.

With every passing day, we learn of new ways cyber operatives are looking to exploit everything from the media we consume to the databases that store voter registration data.

In this country, there is nothing more sacred than the ability to engage in civic activity and cyber criminals are seeking to undermine our democracy.

Furthermore, as I watch the devastation unfold in Texas, Florida, Puerto Rico, and the Virgin Islands—I am reminded of the fragility of our systems. Disrupting the systems we rely on for power, fuel, food, and water can be deadly, regardless of whether it's caused by a cyber attack or a natural disaster.

In short, the digital networks we rely on for our day-to-day life are facing a multitude of threats. To respond to these threats, Congress has put its trust in DHS.

Over the past few years, Congress—by way of this committee—has consistently expanded DHS's cybersecurity mission—giving the Department a key role in securing Federal networks as well as the systems that support our Nation's critical infrastructure.

The Department made huge strides in implementing these new authorities—including by standing up an automated system to share cyber threat data and advising the new Election Infrastructure subsector on how to promote cyber hygiene with election administrators throughout the country.

We cannot, however, expect DHS to carry out these responsibilities with both hands tied behind its back. To be successful, the Department needs adequate resources, a robust staff, strong leadership, and a clear strategy.

Unfortunately, this administration has been gravely unfocused when it comes to cybersecurity. President Trump falsely promised to deliver "a comprehensive plan to protect America's vital infrastructure from cyber attacks" on his first day in office. It took months for the President to get around to issuing an Executive Order on cybersecurity.

Also, a quarter of the 28-person National Infrastructure Advisory Council resigned in protest of President Trump's "insufficient attention" to cyber threats.

President Trump floated the idea of an "impenetrable cyber unit" with Russia at the same time members of his administration were considering—and ultimately decided—to ban the use of Kaspersky products on Federal networks.

Within DHS, the chief information officer resigned after serving only 4 months, and the National Programs and Protection Directorate, the Department's main cyber arm, is still operating without a permanent under secretary.

Whether the men and women in this room are willing to acknowledge, in an open setting, that they are struggling without this leadership—we can be certain these gaps are making their jobs harder.

I look forward to hearing from this panel today about how the Department is carrying out its cyber mission, and I hope that you'll be candid with us about the obstacles you face. If there are areas where you need additional resources or legislative clarity, tell us how we can help.

Mr. RATCLIFFE. I thank the gentlemen. Other Members of the committee are reminded that opening statements may be submitted for the record.

We are pleased to have a distinguished panel of witnesses before us today on this very important topic. Mr. Christopher Krebs is the senior official performing the duties of the under secretary of the National Protection and Programs Directorate at the United States Department of Homeland Security. Great to see you today Mr. Krebs, and great to see you in your new roles at DHS.

Ms. Jeanette Manfra is the assistant secretary for cybersecurity and communications in the National Protection and Programs Directorate at DHS. Also great to have you back before our subcommittee, Ms. Manfra.

Finally Ms. Patricia Hoffman is the acting assistant secretary for the Office of Electricity Delivery and Energy Reliability at the U.S. Department of Energy. Thank you for being here with us today.

I would now like to ask the witnesses to stand and raise your right hand so that I can swear you in to testify.

[Witnesses sworn.]

Mr. RATCLIFFE. Let the record reflect that each of the witnesses has answered in the affirmative. You may be seated. The witnesses' full written statements will appear in the record.

The Chair now recognizes Mr. Krebs for 5 minutes for his opening statement.

STATEMENT OF CHRISTOPHER KREBS, SENIOR OFFICIAL PERFORMING THE DUTIES OF THE UNDER SECRETARY, NATIONAL PROTECTION AND PROGRAMS DIRECTORATE, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. KREBS. Chairman Ratcliffe, Ranking Member Richmond, Ranking Member Thompson, Members of the committee, good morning and thank you for today's hearing.

In this month of October, we recognize National Cybersecurity Awareness Month, a time to focus on how cybersecurity is a shared responsibility that affects all Americans. The Department of Homeland Security serves a critical role in safeguarding and securing cyber space, a core Homeland Security mission.

I want to begin my testimony by thanking the committee for taking action earlier this summer on the Cybersecurity and Infrastructure Security Agency Act of 2017. If enacted, this legislation would mature and streamline the National Protection and Programs Directorate, or NPPD, and rename our organization to clearly reflect our central mission. The Department strongly supports this much-needed effort and encourages swift action by the full House and Senate.

NPPD's mission statement is clear. We lead the Nation's efforts to ensure the security and resilience of our cyber and physical infrastructure. We collaborate with other Federal agencies, State, local, Tribal, and territorial governments and, of course, the private sector.

Our three goals are as follows: Secure and defend Federal networks and facilities; identify and mitigate critical infrastructure systemic risk; incentivize and broadly enable enhanced cyber and physical security practices. No question this is an expansive mission.

As we meet today, I am proud to share with you the tireless efforts of so many at NPPD and in coordination with our interagency partners to accomplish this mission: The targeting of our elections, WannaCry, NotPetya, intrusions into energy and nuclear sector infrastructure, Harvey, Irma, Maria, soft-target attacks in London, Barcelona, Orlando, and most recently, Las Vegas.

As threats to our critical infrastructure evolve and in many ways remain the same, our people are partnering with owners and operators across America. We are engaging the public to raise awareness because our security is truly a shared responsibility.

Today's hearing is about DHS's cybersecurity mission. Earlier this year the President signed an Executive Order on strengthening the cybersecurity of Federal networks and critical infrastructure. This Executive Order set in motion a series of these assessments and deliverables to improve our defenses and lower our risks to cyber threats.

DHS is organized around these deliverables by working with Federal and private-sector partners. We are emphasizing the security of Federal networks. Across the Federal Government, agencies have been implementing the industry standard NIST cybersecurity framework.

Agencies are reporting to DHS and the Office of Management and Budget, or OMB, on their cybersecurity risk management and mitigation acceptance choices. DHS and OMB are evaluating the totality of these agency reports in order to comprehensively assess the adequacy of the Federal Government's overall cybersecurity risk management posture.

In addition to our efforts to protect Federal Government networks, we are focused on how Government and industry work together to protect the Nation's critical infrastructure. We are prioritizing deeper, more collaborative public-private relationships and partnerships.

In collaboration with civilian, military, and intelligence agencies, we are developing an inventory of authorities and capabilities. We are prioritizing entities at greatest risk of attacks that could result in catastrophic consequences. We commonly call this our Section 9 efforts.

Before closing, let me also discuss our continued efforts to address cybersecurity risks facing our election infrastructure. Facing the threat of cyber-enabled operations by a foreign government during the 2016 elections, DHS and our interagency partners conducted unprecedented outreach and provided cybersecurity assistance to State and local election officials. Information shared included indicators of compromise, technical data, and best practices.

Through numerous efforts before and after election day, we declassified and shared information related to Russian malicious cyber activity. These steps have been critical to protecting our elections, enhancing awareness among election officials, and educating the American public.

The designation of election infrastructure as critical infrastructure provides a foundation to institutionalize and prioritize services and support. We are working with Federal, State, and local partners to develop information, sharing protocols and establish key working groups. Yet there is more to be done and we shall not waiver.

In the face of increasingly sophisticated threats, NPPD is focused on defending our Nation's critical infrastructure. The risks are complex and dynamic with interdependencies. Technological advances, such as the internet of things, and cloud computing, increased access, and streamlined efficiencies.

However, they also increase access points that could be leveraged by adversaries to gain unauthorized access to networks. As new threats emerge and our use of technology evolves, we must integrate cyber and physical risk in order to effectively secure our Nation. Expertise around cyber physical risk and cross-sector critical infrastructure interdependencies is where NPPD brings unique expertise and capabilities.

Thank you for inviting me here today, and I look forward to your questions.

[The joint prepared statement of Mr. Krebs and Ms. Manfra follows:]

JOINT PREPARED STATEMENT OF CHRISTOPHER KREBS AND JEANETTE MANFRA

OCTOBER 3, 2017

Chairman Ratcliffe, Ranking Member Richmond, and Members of the committee, thank you for the opportunity to be here today. In this month of October, we recognize National Cybersecurity Awareness Month, a time to focus on how cybersecurity is a shared responsibility that affects all Americans. The Department of Homeland Security (DHS) serves a critical role in safeguarding and securing cyber space, a core homeland security mission. The administration recognizes the committee's work to provide DHS with the authorities necessary to carry out this mission. The National Protection and Programs Directorate (NPPD) at DHS leads the Nation's efforts to ensure the security and resilience of our cyber and physical infrastructure. Earlier this year, this committee voted favorably on H.R. 3359, the "Cybersecurity and Infrastructure Security Agency Act of 2017." If enacted, this bill would mature and streamline NPPD, and rename our organization to clearly reflect our essential mission and our role in securing cyber space. The Department strongly supports this much-needed effort and encourages swift action by the full House and the Senate.

NPPD is responsible for protecting civilian Federal Government networks and collaborating with other Federal agencies, as well as State, local, Tribal, and territorial governments, and the private sector to defend against cyber threats. We endeavor to enhance cyber threat information sharing across the globe to stop cyber incidents before they start and help businesses and Government agencies to protect their cyber systems and quickly recover should such an attack occur. By bringing together all levels of government, the private sector, international partners, and the public, we are taking action to protect against cybersecurity risks, improve our whole-of-Government incident response capabilities, enhance information sharing on best practices and cyber threats, and to strengthen resilience.

THREATS

Cyber threats remain one of the most significant strategic risks for the United States, threatening our National security, economic prosperity, and public health and safety. The past year has marked a turning point in the cyber domain, at least in the public consciousness. We have long been confronted with a myriad of attacks against our digital networks. But over the past year, Americans saw advanced persistent threat actors, including hackers, cyber criminals, and nation-states, increase the frequency and sophistication of these attacks. Our adversaries have been developing and using advanced cyber capabilities to undermine critical infrastructure, target our livelihoods and innovation, steal our National security secrets, and threaten our democracy through attempts to manipulate elections.

Global cyber incidents, such as the "WannaCry" ransomware incident in May of this year and the "NotPetya" malware incident in June, are examples of malicious actors leveraging cyber space to create disruptive effects and cause economic loss. These incidents exploited known vulnerabilities in software commonly used across the globe. Prior to these events, NPPD had already taken actions to help protect networks from similar types of attacks. Through requested vulnerability scanning, NPPD helped stakeholders identify vulnerabilities on their networks so they could be patched before incidents and attacks occur. Recognizing that not all users are able to install patches immediately, NPPD shared additional mitigation guidance to assist network defenders. As the incidents unfolded, NPPD led the Federal Government's incident response efforts, working with our interagency partners, including providing situational awareness, information sharing, malware analysis, and technical assistance to affected entities.

Historically, cyber actors have strategically targeted critical infrastructure sectors including energy, financial services, critical manufacturing, water and wastewater, and others with various goals ranging from cyber espionage to developing the ability to disrupt critical services. In recent years, DHS has identified and responded to malware such as "Black Energy" and "Havex," which were specifically created to target industrial-control systems, associated with critical infrastructure such as power plants and critical manufacturing. More recently, the discovery of "CrashOverride" malware, reportedly used against Ukrainian power infrastructure in 2016, highlights the increasing cyber threat to our infrastructure.

In one recent campaign, advanced persistent threat actors targeted the cyber infrastructure of entities within the energy, nuclear, critical manufacturing, and other critical infrastructure sectors since at least May 2017. In response, NPPD led the asset response, providing on-site and remote assistance to impacted entities, help them evaluate the risk, and remediate the malicious actor presence. In addition, NPPD, the Federal Bureau of Investigation, and the Department of Energy (DOE) shared actionable analytic products with critical infrastructure owners and operators regarding this activity. This information provides network defenders with the information necessary to understand the adversary campaign and allows them to identify and reduce exposure to malicious activity. In addition, DHS has been working together with DOE to assess the preparedness of our electricity sector and strengthen our ability to respond to and recover from a prolonged power outage caused by a cyber incident.

CYBERSECURITY PRIORITIES

Earlier this year, the President signed Executive Order (EO) 13800, on *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*. This Executive Order set in motion a series of assessments and deliverables to understand how to improve our defenses and lower our risk to cyber threats. DHS has organized around these deliverables, working with Federal and private-sector partners to work through the range of actions included in the Executive Order.

We are emphasizing the security of Federal networks. Across the Federal Government, agencies have been implementing action plans to use the industry-standard Department of Commerce's National Institute of Standards and Technology Cybersecurity Framework. Agencies are reporting to DHS and the Office of Management and Budget (OMB) on their cybersecurity risk mitigation and acceptance choices. In coordination with OMB, DHS is evaluating the totality of these agency reports in order to comprehensively assess the adequacy of the Federal Government's overall cybersecurity risk management posture.

Although Federal agencies have primary responsibility for their own cybersecurity, DHS, pursuant to its various authorities, provides a common set of security tools across the civilian Executive branch and helps Federal agencies manage their cyber risk. NPPD's assistance to Federal agencies includes: (1) Providing tools to safeguard civilian Executive branch networks through the National Cybersecurity Protection System (NCPS), which includes "EINSTEIN", and the Continuous Diagnostics and Mitigation (CDM) programs, (2) measuring and motivating agencies to implement policies, directives, standards, and guidelines, (3) serving as a hub for information sharing and incident reporting, and (4) providing operational and technical assistance, including threat information dissemination and risk and vulnerability assessments, as well as incident response services. NPPD's National Cybersecurity and Communications Integration Center (NCCIC) is the civilian government's hub for cybersecurity information sharing, asset incident response, and coordination for both critical infrastructure and the Federal Government.

EINSTEIN refers to the Federal Government's suite of intrusion detection and prevention capabilities that protects agencies' Unclassified networks at the perimeter of each agency. EINSTEIN provides situational awareness of civilian Executive branch network traffic, so threats detected at one agency are shared with all others providing agencies with information and capabilities to more effectively manage their cyber risk. The U.S. Government could not achieve such situational awareness through individual agency efforts alone.

Today, EINSTEIN is a signature-based intrusion detection and prevention capability that takes action on known malicious activity. Leveraging existing investments in the Internet Service Provider "ISP" infrastructure, our non-signature based pilot efforts to move beyond current reliance on signatures are yielding positive results in the discovery of previously-unidentified malicious activity. DHS is demonstrating the ability to capture data that can be rapidly analyzed for anomalous activity using technologies from commercial, Government, and open sources. The pilot efforts are also defining the future operational needs for tactics, techniques, and procedures as well as the skill sets and personnel required to operationalize the non-signature-based approach to cybersecurity.

State, local, Tribal, and territorial governments are able to access intrusion detection and analysis services through the Multi-State Information Sharing and Analysis Center (MS–ISAC). MS–ISAC's service, called "Albert," closely resembles some EINSTEIN capabilities. While the current version of Albert cannot actively block known cyber threats, it does alert cybersecurity officials to an issue for further investigation. DHS worked closely with MS–ISAC to develop the program and considers MS–ISAC to be a principal conduit for sharing cybersecurity information with State and local governments.

EINSTEIN, the Federal Government's tool to address perimeter security will not block every threat; therefore, it must be complemented with systems and tools working inside agency networks—as effective cybersecurity risk management requires a defense-in-depth strategy that cannot be achieved through only one type of tool. NPPD's Continuous Diagnostics and Mitigation (CDM) program provides cybersecurity tools and integration services to all participating agencies to enable them to improve their respective security postures by reducing the attack surface of their networks as well as providing DHS with enterprise-wide visibility through a common Federal dashboard.

CDM is helping us achieve two major advances for Federal cybersecurity. First, agencies are gaining visibility, often for the first time, into the extent of cybersecurity risks across their entire network. With enhanced visibility, they can prioritize the mitigation of identified issues based upon their relative importance. Second, with the summary-level agency-to-Federal dashboard feeds, the NCCIC will be able to identify systemic risks across the civilian Executive branch more effectively and closer to real-time. For example, the NCCIC currently tracks Government-wide progress in implementing critical patches via agency self-reporting and manual data calls. CDM will transform this, enabling the NCCIC to immediately view the prevalence of a given software product or vulnerability across the Federal Government so that the NCCIC can provide agencies with timely guidance on their risk exposure and recommended mitigation steps. Effective cybersecurity requires a robust measurement regime, and robust measurement requires valid and timely data. CDM will provide this baseline of cybersecurity risk data to drive improvement across the civilian Executive branch.

DHS conducts a number of activities to measure agencies' cybersecurity practices and works with agencies to improve risk management practices. The Federal Information Security Modernization Act of 2014 (FISMA) provided the Secretary of Homeland Security with the authority to develop and oversee implementation of Binding Operational Directives (BOD) to agencies. In 2016, the Secretary issued a BOD on securing High-Value Assets (HVA), or those assets, Federal information systems, information, and data for which unauthorized access, use, disclosure, disruption, modification, or destruction could cause a significant impact to the United States' National security interests, foreign relations, economy, or to the public confidence, civil liberties, or public health and safety of the American people. NPPD works with interagency partners to prioritize HVAs for assessment and remediation activities across the Federal Government. For instance, NPPD conducts security architecture reviews on these HVAs to help agencies assess their network architecture and configurations.

As part of the effort to secure HVAs, DHS conducts in-depth vulnerability assessments of prioritized agency HVAs to determine how an adversary could penetrate a system, move around an agency's network to access sensitive data, and exfiltrate such data without being detected. These assessments include services such as penetration testing, wireless security analysis, and "phishing" evaluations in which DHS hackers send emails to agency personnel and test whether recipients click on potentially malicious links. DHS has focused these ssessments on Federal systems that may be of particular interest to adversaries or support uniquely significant data or services. These assessments provide system owners with recommendations to address identified vulnerabilities. DHS provides these same assessments, on a voluntary basis upon request, to private sector and State, local, Territorial, and Tribal (SLTT) partners. DHS also works with the General Services Administration to ensure that contractors can provide assessments that align with our HVA initiative to agencies.

Another BOD issued by the Secretary directs civilian agencies to promptly patch known vulnerabilities on their internet-facing systems that are most at risk from their exposure. The NCCIC conducts Cyber Hygiene scans to identify vulnerabilities in agencies' internet-accessible devices and provides mitigation recommendations. Agencies have responded quickly in implementing the Secretary's BOD and have sustained this progress. When the Secretary issued this directive, NPPD identified more than 360 "stale" critical vulnerabilities across Federal civilian agencies, which means the vulnerabilities had been known for at least 30 days and remained unpatched. Since December 2015, NPPD has identified an average of less than 40 critical vulnerabilities at any given time, and agencies have addressed those vulnerabilities rapidly once they were identified. By conducting vulnerability assessments and security architecture reviews, NPPD is helping agencies find and fix vulnerabilities and secure their networks before an incident occurs.

In addition to efforts to protect Government networks, EO 13800 continues to examine how the Government and industry work together to protect our Nation's critical infrastructure, prioritizing deeper, more collaborative public-private partnerships in threat assessment, detection, protection, and mitigation. In collaboration with civilian, defense, and intelligence agencies, we are identifying authorities and capabilities that agencies could employ, soliciting input from the private sector, and developing recommendations to support the cybersecurity efforts of those critical infrastructure entities at greatest risk of attacks that could result in catastrophic impacts.

For instance, by sharing information quickly and widely, we help all partners block cyber threats before damaging incidents occur. Equally important, the information we receive from partners helps us identify emerging risks and develop effective protective measures.

Congress authorized the NCCIC as the civilian hub for sharing cyber threat indicators and defensive measures with and among Federal and non-Federal entities, including the private sector. As required by the Cybersecurity Act of 2015, we established a capability, known as Automated Indicator Sharing (AIS), to automate our sharing of cyber threat indicators in real-time. AIS protects the privacy and civil liberties of individuals by narrowly tailoring the information shared to that which is necessary to characterize identified cyber threats, consistent with longstanding DHS policy and the requirements of the Act. AIS is a part of the Department's effort to create an environment in which as soon as a company or Federal agency observes an attempted compromise, the indicator is shared in real time with all of our partners, enabling them to protect themselves from that particular threat. This real-time sharing capability can limit the scalability of many attack techniques, thereby increasing the costs for adversaries and reducing the impact of malicious cyber activity. An ecosystem built around automated sharing and network defense-in-depth should enable organizations to detect and thwart the most common cyber attacks, freeing their cybersecurity staff to concentrate on the novel and sophisticated attacks. More than 129 agencies and private-sector partners have connected to the AIS capability. Notably, partners such as information sharing and analysis organizations (ISAOs) and computer emergency response teams further share with or protect their customers and stakeholders, significantly expanding the impact of this capability. AIS is still a new capability and we expect the volume of threat indicators shared through this system to substantially increase as the technical standards, software, and hardware supporting the system continue to be refined and put into full production. As more indictors are shared from other Federal agencies, SLTT governments, and the private sector, this information-sharing environment will become more robust and effective.

Another part of the Department's overall information-sharing effort is to provide Federal network defenders with the necessary context regarding cyber threats to prioritize their efforts and inform their decision making. DHS's Office of Intelligence and Analysis (I&A) has collocated analysts within the NCCIC responsible for continuously assessing the specific threats to Federal networks using traditional all-source methods and indicators of malicious activity so that the NCCIC can share with Federal network defenders in collaboration with I&A. Analysts and personnel from the Department of Energy, Treasury, Health and Human Services, FBI, DoD, and others are also collocated within the NCCIC and working together to understand the threats and share information with their sector stakeholders.

MITIGATING CYBER RISKS

We also continue to adapt to the evolving risks to critical infrastructure, and prioritize our services to mitigate those risks. Facing the threat of cyber-enabled operations by a foreign government during the 2016 elections, DHS and our interagency partners conducted unprecedented outreach and provided cybersecurity assistance to State and local election officials. Information shared with election officials included indicators of compromise, technical data, and best practices that have assisted officials with addressing threats and vulnerabilities related to election infrastructure. Through numerous efforts before and after Election Day, DHS and our interagency partners have declassified and publicly shared significant information related to the Russian malicious cyber activity. These steps have been critical to protecting our elections, enhancing awareness among election officials, and educating the American public. The designation of election infrastructure as critical infrastructure serves to institutionalize prioritized services, support, and provide data protections and does not subject any additional regulatory oversight or burdens.

As the Sector-Specific Agency, NPPD is providing overall coordination guidance on election infrastructure matters to subsector stakeholders. As part of this process, the

Election Infrastructure Subsector Government Coordinating Council (GCC) is being established. The Election Infrastructure Subsector GCC will be a representative council of Federal, State, and local partners with the mission of focusing on sector-specific strategies and planning. This will include development of information-sharing protocols and establishment of key working groups, among other priorities.

The Department also recently took action against specific products which present a risk to Federal information systems. After careful consideration of available information and consultation with interagency partners, last month the Acting Secretary issued a BOD directing Federal Executive branch departments and agencies to take actions related to the use or presence of information security products, solutions, and services supplied directly or indirectly by AO Kaspersky Lab or related entities. The BOD calls on departments and agencies to identify any use or presence of Kaspersky products on their information systems in the next 30 days, to develop detailed plans to remove and discontinue present and future use of the products in the next 60 days, and at 90 days from the date of this directive, unless directed otherwise by DHS based on new information, to begin to implement the agency plans to discontinue use and remove the products from information systems. This action is based on the information security risks presented by the use of Kaspersky products on Federal information systems.

The Department is providing an opportunity for Kaspersky to submit a written response addressing the Department's concerns or to mitigate those concerns. The Department wants to ensure that the company has a full opportunity to inform the Acting Secretary of any evidence, materials, or data that may be relevant. This opportunity is also available to any other entity that claims its commercial interests will be directly impacted by the directive.

CONCLUSION

In the face of increasingly sophisticated threats, NPPD stands on the front lines of the Federal Government's efforts to defend our Nation's critical infrastructure from natural disasters, terrorism and adversarial threats, and technological risk such as those caused by cyber threats. Our infrastructure environment today is complex and dynamic with interdependencies that add to the challenge of securing and making it more resilient. Technological advances have introduced the "internet of things" (IoT) and cloud computing, offering increased access and streamlined efficiencies, while increasing our footprint of access points that could be leveraged by adversaries to gain unauthorized access to networks. As our Nation continues to evolve and new threats emerge, we must integrate cyber and physical risk in order to understand how to effectively secure it. Expertise around cyber-physical risk and cross-sector critical infrastructure interdependencies is where NPPD brings unique expertise and capabilities.

We must ensure that NPPD is appropriately organized to address cybersecurity threats both now and in the future, and we appreciate this committee's leadership in working to establish the Cybersecurity and Infrastructure Security Agency. As the committee considers these issues, we are committed to working with Congress to ensure that this effort is done in a way that cultivates a safer, more secure, and resilient homeland.

Thank you for the opportunity to testify, and we look forward to any questions you may have.

Mr. RATCLIFFE. Thank you, Mr. Krebs.

Ms. Manfra you are now recognized for 5 minutes.

STATEMENT OF JEANETTE MANFRA, ASSISTANT SECRETARY FOR CYBERSECURITY AND COMMUNICATIONS, NATIONAL PROTECTION AND PROGRAMS DIRECTORATE, U.S. DEPARTMENT OF HOMELAND SECURITY

Ms. MANFRA. Chairman Ratcliffe, Ranking Member Richmond, Ranking Member Thompson, Members of the committee, thank you for holding today's hearing.

I also want to begin my testimony by thanking this committee for taking action earlier this summer of the Cybersecurity and Infrastructure Security Agency Act of 2017. A name for our organization that reflects our mission is essential to our work force recruitment efforts and effective stakeholder engagement.

We must also ensure that NPPD is appropriately organized to address cybersecurity threats, both now and in the future, and we appreciate this committee's leadership.

Cyber threats remain one of the most significant strategic risks for the United States. Cyber risks threaten our National security, economic prosperity, and public health and safety. Our adversaries cross borders at the speed of light.

Over the past year Americans saw advanced persistent threat actors, including hackers, criminals, and nation-states increase in frequency, complexity, and sophistication. In my role at DHS, I head the Department's Office of Cybersecurity and Communications, which includes our 24/7 watch center and operations at the National Cybersecurity and Communications Integration Center.

Our role goes along three work streams: Instrumenting agency networks through the deployment of sensors; assessing and measuring agency vulnerabilities and risks, as well as critical infrastructure; and directing and advising actions that Federal agencies and critical infrastructure entities can take to better secure their networks.

As you well know, the NCCIC is a civilian-Government hub for cybersecurity information sharing, asset incident response, and coordination for both critical infrastructure and the Federal Government.

As my colleague noted, we are emphasizing the security of Federal networks. NPPD's assistance to Federal agencies includes first providing tools to safeguard civilian Executive branch networks through our National cyber protection system and the continuous diagnostics and mitigation programs; second, measuring and motivating agencies; and third, serving as a hub for information sharing and incident reporting; and finally, providing operational and technical assistance.

Einstein, the sensors deployed as a part of the National cyber protection system, refers to the Federal Government's suite of intrusion detection and prevention capabilities that protects the agencies' Unclassified networks at the perimeter of each agency. Today Einstein is a signature-based intrusion protection and prevention capability that takes action on known malicious activity.

Our non-signature-based pilot efforts to move beyond signatures are yielding positive results. These capabilities are essential to discovery of previously-unidentified malicious activity. We are demonstrating the ability to capture data that can rapidly be analyzed for anomalous activity, using technologies from commercial, Government, and open sources.

The pilot efforts are also defining the future operational needs for tactics, techniques, and procedures, as well as the skill sets and personnel required to operationalize the non-signature-based approach to cybersecurity.

Einstein is our tool to address perimeter security, but it will not detect or block every threat. Therefore we must complement it with systems and tools working inside agency networks.

Our continuous diagnostics and mitigation program provides those tools and integration services to Federal agencies. These tools are enabling agencies to manage risks across their entire enterprise. At the same time, these tools are also going to provide DHS visibility into our enterprise risk across the Federal Government through a common Federal dashboard.

NPPD is also working with our interagency partners to prioritize high-value assets, or those systems for which a cyber incident could cause a significant impact to the United States.

As part of this effort, we conduct security architecture reviews to help agencies assess their network architecture and configurations. We conduct in-depth vulnerability assessments of these prioritized assets to determine how an adversary would penetrate a system, move around an agency's network to access sensitive data, and exfiltrate such data without being detected.

These assessments provide system owners with recommendations to address identified vulnerabilities, protecting them before an incident occurs.

When necessary, the Department also is also taking targeted action to address specific cybersecurity risks through the issuance of binding operational directives. We are working to enhance cyber threat information sharing across the globe to stop cyber incidents before they start.

These actions help businesses and Government agencies protect their systems and quickly recover should such an attack occur. By bringing together all levels of government, the private sector, international partners, and the public, we are taking action to protect against cybersecurity risks, improve our whole-of-Government incident response capabilities, enhance information sharing on best practices and cyber threats, and to strengthen resilience.

Thank you for the opportunity to testify and I look forward to any questions you may have.

Mr. RATCLIFFE. Thanks, Ms. Manfra.

Ms. Hoffman you are recognized for 5 minutes.

STATEMENT OF PATRICIA HOFFMAN, ACTING ASSISTANT SECRETARY, OFFICE OF ELECTRICITY DELIVERY AND ENERGY RELIABILITY, U.S. DEPARTMENT OF ENERGY

Ms. HOFFMAN. Chairman Ratcliffe, Ranking Member Richmond, and Members of the subcommittee, thank you for the opportunity to discuss the continuing threats facing our Nation's energy infrastructure, and the Department of Energy's role.

Cybersecurity and resilience of the energy sector is one of the Secretary's top priorities and a major focus of the Department. The Department of Energy is the sector-specific agency for cybersecurity of the energy sector.

DOE works with DHS and jointly with other agencies, the private-sector organizations, for a whole-of-Government response to cyber incidents by protecting assets and countering threats.

In addition, the Department of Energy serves as the lead agency for Emergency Support Function 12, which is energy, under the National response framework. As a lead, ESF 12 is responsible for facilitating restoration of damaged energy infrastructure. The Department works with industry, Federal, State, and local partners to facilitate response and recoveries.

Combining DOE's role as the SSA for cybersecurity with National response activity, ensures that incidents, both cyber and physical, impacts are coordinated in the energy sector.

At this moment in time I would like to acknowledge that the Secretary does express his support for the victims of Hurricanes Harvey, Irma, and Maria, and I would also like to express my gratitude for all the utility workers that have been working very hard in the regions for restoring power.

In extreme cases the Department can also use its legal authorities, as those in the Federal Power Act as amended by the Fixing America's Service Transportation Act, to assist in response and recovery operations. Congress enacted several important new energy security measures in this act as it relates to cybersecurity.

The Secretary of Energy was provided a new authority upon declaration of a grid security emergency by the President, to issue emergency orders to protect or restore critical electric infrastructure, or defense critical electric infrastructure. This authority allows DOE to respond as needed to the threat of cyber and physical attacks to the grid.

DOE has collaborated with the energy sector for nearly two decades in voluntary public-private partnerships that engage owners and operators at all levels, technical, operational, and executive, along with State and local governments, to identify and mitigate physical and cyber risks to the energy systems.

In the energy sector, the core partnerships have consisted with the electric sector coordinating council and the oil and gas coordinating council. In these meetings, interagency partners, including DHS, States, international partners come together to discuss important security and resilience issues for the energy sector.

The electric sector, specifically, has been very forward-leaning and aggressive in trying to address cybersecurity issues. DOE plays a critical role in supporting the energy sector's cybersecurity by building in security.

Specifically we have been looking at building capabilities in the sectors in three areas. The first area is preparedness, enhancing the visibility and situational awareness in operational networks as well as I.T. networks, increasing the alignment of cybersecurity preparedness across multiple States and Federal jurisdictions, response and recovery activities, and supporting the whole-of-Government effort, and leveraging the expertise of the Department of Energy's National labs to drive cybersecurity innovation.

Threats continue to evolve. DOE is working diligently to stay ahead of the curve. The solution is an ecosystem of resilience that works in partnership with State, local, and industry stakeholders to advance best practices, strategies, and tools.

To accomplish this we must accelerated information sharing to better inform local investment decisions, encourage innovation, and the use of best practices to help raise the energy sector's security maturity and strengthen local incident response and recovery activities, especially through the participation in training programs and exercises.

I appreciate the opportunity to be here before the subcommittee and represent one of the sector's specific agencies and the energy sector's cybersecurity capabilities.

However I would be remiss not to take a moment and stress the interdependent nature of our infrastructure. It requires all sectors to be constantly focused on improving their cybersecurity posture.

So DOE looks forward to continue working with the Federal agencies to share best practices and build a defense in-depth.

So with that I would like to thank you for being here today and look forward to answering your questions.

[The prepared statement of Ms. Hoffman follows:]

Prepared Statement of Patricia Hoffman

October 3, 2017

INTRODUCTION

Chairman Ratcliffe, Ranking Member Richmond, and Members of the subcommittee, thank you for the opportunity to discuss the continuing threats facing our National energy infrastructure and the Department of Energy's (DOE's) role in supporting the cybersecurity of the Nation's energy infrastructure. Cybersecurity and the resilience of the energy sector is one of the Secretary's top priorities and a major focus of the Department.

Our economy, National security, and even the well-being of our citizens depend on the reliable delivery of electricity. The mission of the Office of Electricity Delivery and Energy Reliability (DOE–OE)—which I oversee in my roles as the acting under secretary for science and energy and acting assistant secretary for DOE–OE—is to strengthen, transform, and improve energy infrastructure to ensure access to reliable and secure sources of energy. The Secretary of Energy and DOE are committed to working with our public and private-sector partners to protect the Nation's critical energy infrastructure from physical security events, natural and man-made disasters, and cybersecurity threats.

DOE'S ROLE AS THE ENERGY SECTOR'S "SECTOR-SPECIFIC AGENCY"

In preparation for, and response to, cybersecurity threats, the Federal Government's operational framework is provided by Presidential Policy Directive 41 (PPD–41). A primary purpose of PPD–41 is to clarify the roles and responsibilities of the Federal Government during a "significant cyber incident," which are described as cyber incidents that are "likely to result in demonstrable harm to the National security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people."

Under the PPD–41 framework, as the Sector-Specific Agency (or SSA) for cybersecurity of the energy sector, DOE works jointly with other agencies and private-sector organizations, including the Federal Government's designated lead agencies for coordinating the response to significant cyber incidents by protecting assets and countering threats: The Department of Homeland Security (DHS) acting through the National Cybersecurity and Communications Integration Center (NCCIC) and the Department of Justice (DOJ), acting through the Federal Bureau of Investigation (FBI) and the National Cyber Investigative Joint Task Force, respectively. In the event of a cybersecurity emergency in the energy sector, closely aligning DOE's activities with those of our partners at DHS and DOJ helps to ensure that DOE's deep expertise with the sector is appropriately leveraged.

Under *Presidential Policy Directive–21 (PPD–21): Critical Infrastructure Security and Resilience*, later codified in part in the Fixing America's Surface Transportation Act, DOE is designated as the SSA for cybersecurity of the energy sector. As the SSA, DOE coordinates with DHS and other Federal agencies and collaborates with industry and State, local, Tribal, and territorial partners on matters of cyber resilience, incident response, and planning. For any risk to the energy sector, DOE thus acts to ensure unity of effort across government, including States, and industry partners.

In addition, DOE serves as the lead agency for Emergency Support Function 12 (ESF–12) under the National Response Framework. As the lead for ESF–12, DOE is responsible for facilitating the restoration of damaged energy infrastructure. The Department works with industry and Federal, State, and local partners to facilitate response and recovery. Combining DOE roles as the SSA in cybersecurity with National response ensures incidents with both cyber and physical impacts can be coordinated for the energy sector.

In extreme cases, the Department can use its legal authorities such as those in the Federal Power Act, as amended by the Fixing America's Surface Transportation (FAST) Act, to assist in response and recovery operations. Congress enacted several important new energy security measures in the FAST Act as it relates to cybersecurity. The Secretary of Energy was provided a new authority, upon declaration of a

"Grid Security Emergency" by the President, to issue emergency orders to protect or restore critical electric infrastructure or defense critical electric infrastructure. This authority allows DOE to respond as needed to the threat of cyber and physical attacks on the grid.

DOE is working to address public comments received regarding the rules of procedure to issue an order under this new authority. The Grid Security Emergency authority is unique to DOE and an important element in partnering with DHS and DOJ to fully address the cybersecurity risks to the energy sector.

THE SPECIAL NATURE OF ENERGY SECURITY CYBERSECURITY

Cyber attacks targeting "information technology" or IT, including computing and business applications, to cause disruptions, obtain access to email accounts and personal information, exfiltrate data to release to the world at large, and exploit information for private gain are growing increasingly common. The energy sector is not immune to such attacks.

However, our adversaries understand that the energy sector is a valuable target not because of its IT systems, but because of the assets that the sector controls. Accordingly, we have seen an increased interest in vulnerabilities of the "operating technology," or OT, of energy delivery systems and other critical infrastructure as well. OT systems consist of industrial control systems (or ICS), programmable logic controls, and its associated supervisory control and data acquisition software (known as SCADA). The heavy use of OT systems has made electric utilities, oil and natural gas providers, hydro and nuclear facilities, and water utilities prime targets for OT-related cyber attacks. The disruption of any one of these is not only inherently problematic, it also hampers the ability to respond to any type of emergency event.

The Department's focus on OT systems specific to the energy sector makes our activities both distinct from, and complementary to, the activities of DHS and our other Federal agency partners. The cybersecurity of energy sector OT systems requires specific and focused attention because of their need for extremely high reliability and availability, the fact that any significant reduction in the speed of the systems is unacceptable, and because these systems are so critical to underpinning the Nation's economic health, public safety, and National security.

In December 2015, the first known successful cyber attack on power grid OT took place in Ukraine. Over 225,000 residents were left without power for several hours in the coordinated attack, and a second attack occurred in December 2016 that left portions of Kiev without electricity. More recently, publicly-available information about threats such as the Crash Override malware used in Ukraine and the nation-state activities described under the name "Dragonfly 2.0" are just two of many examples that illustrate the threat to the Nation's energy infrastructure is real and growing more concerning by the day.

IMPORTANCE OF PARTNERSHIPS

Before I describe the details of the Department's activities in support of the energy sector's cybersecurity, I must first focus on the most foundational aspect of our activities: Partnerships. The Federal Government does not own or operate the vast majority of the assets in the Nation's energy sector, and DOE does not hold a monopoly on protecting the Nation's critical infrastructure from cyber threats. As such, we cannot function effectively unless we have strong partnerships throughout the public and private sectors and with our Federal colleagues at DHS and other law enforcement- and National security-oriented agencies.

DOE has collaborated with the energy sector for nearly two decades in voluntary public-private partnerships that engage energy owners and operators at all levels—technical, operational, and executive, along with State and local governments—to identify and mitigate physical and cyber risks to energy systems.

These partnerships are built on a foundation of earned trust that promotes the mutual exchange of information and resources to improve the security and resilience of critical energy infrastructures. These relationships acknowledge the special security challenges of energy delivery systems and leverage the distinct technical expertise within industry and Government to develop solutions.

The security and integrity of energy infrastructure is both a State and Federal Government concern because energy underpins the operations of every other type of critical infrastructure; the economy; and public health and safety. The owners and operators of energy infrastructure, however, have the primary responsibility for the full spectrum of cybersecurity risk management: Identify assets, protect critical systems, detect incidents, respond to incidents, and recover to normal operations.

When the lights go out or gasoline stops flowing in pipelines, the first responder is usually not the State or Federal Government but, rather, industry or local government. This is why public-private partnerships regarding cybersecurity are paramount—they recognize the distinct roles and capabilities of industry and Government in managing our critical energy infrastructure risks.

In the Energy Sector, the core of critical infrastructure partners consists of the Electricity Subsector Coordinating Council (ESCC), the Oil and Natural Gas Subsector Coordinating Council (ONG SCC), and the Energy Government Coordinating Council (EGCC). The ESCC and ONG SCC represent the interests of their respective industries. The EGCC, led by DOE and co-chaired with DHS, is where the interagency partners, States, and international partners come together to discuss the important security and resilience issues for the energy sector. This forum ensures that we're working together in a whole-of-Government response.

As defined in the National Infrastructure Protection Plan, the industry coordinating councils or "SCCs" are created by owners and operators and are self-organized, self-run, and self-governed, with leadership designated by the SCC membership. The SCCs serve as the principal collaboration points between the Government and private-sector owners and operators for critical infrastructure security and resilience coordination and planning, as well as a range of sector-specific activities and issues.

The SCCs, EGCC, and associated working groups operate under DHS's Critical Infrastructure Partnership Advisory Council (CIPAC) framework, which provides a mechanism for industry and Government coordination. The public-private critical infrastructure community engages in open dialog to mitigate critical infrastructure vulnerabilities and to help reduce impacts from threats.

DOE'S CYBERSECURITY STRATEGY FOR THE ENERGY SECTOR

To address these challenges, it is critical for us to be proactive and cultivate what I call an ecosystem of resilience: A network of producers, distributors, regulators, vendors, and public partners, acting together to strengthen our ability to prepare, respond, and recover. We continue to partner with industry, DHS and other Federal agencies, States, local governments, and energy stakeholders broadly to quickly identify threats, develop capabilities to support mitigation strategies, and rapidly respond to any disruptions.

DOE plays a critical role in supporting energy sector cybersecurity to enhance the security and resilience of the Nation's energy infrastructure. As part of a comprehensive strategy for energy resilience, the Department is focusing cyber support efforts to: Enhance visibility and situational awareness of operational networks; increase alignment of cyber preparedness and planning across local, State, and Federal levels; and leverage the expertise of DOE's National Labs to drive cybersecurity innovation.

Enhance visibility and situational awareness of operational networks

It is necessary for partners in the Energy Sector and the Government to share emerging threat data and vulnerability information to help prevent, detect, identify, and thwart cyber attacks more rapidly. An example of this type of collaboration is the Cybersecurity Risk Information Sharing Program (CRISP), a voluntary public-private partnership that is primarily funded by industry, administered by the Electricity Information Sharing and Analysis Center (E–ISAC), and enhanced by DOE through intelligence analysis by DOE's Office of Intelligence and Counterintelligence. One of DOE's National Laboratories—the Pacific Northwest National Laboratory—is a key partner for the E–ISAC in accomplishing the goals of the CRISP program.

The purpose of CRISP is to share information among electricity subsector partners, DOE, and the intelligence community to facilitate the timely bi-directional sharing of Unclassified and Classified threat information to enhance the sector's ability to identify, prioritize, and coordinate the protection of critical infrastructure and key resources. CRISP leverages advanced sensors and threat analysis techniques developed by DOE along with DOE's expertise as part of the intelligence community to better inform the energy sector of the high-level cyber risks. Current CRISP participants provide power to over 75 percent of the total number of continental United States electricity customers. The Department is currently in the early stages of taking the lessons learned from CRISP and developing an analogous capability to monitor network traffic on OT networks.

If CRISP has demonstrated one finding to DOE, the E–ISAC, and our industry partners, it is that continuous monitoring of critical networks and shared situational awareness is of utmost importance in protecting against malicious cyber activities.

Programs such as CRISP are critical for facilitating the identification of and response to advanced persistent threats targeting the energy sector.

Advancing this project to improve situational awareness of OT networks is a key focus of DOE's current activities. Observing anomalous traffic on networks—and having the ability to store and retrieve network traffic from the recent past—can be the first step in stopping an attack early in the cyber kill chain. Continuous monitoring of IT and OT networks, in coordination with Federal partners and industry, is a critical component of protecting the Nation against cyber threats.

Increase alignment of cyber preparedness and planning across local, State, and Federal levels

As the Energy SSA, DOE works at many levels of the electricity, petroleum, and natural gas industries. We interact with numerous stakeholders and industry partners to share both Classified and Unclassified information, discuss coordination mechanisms, and promote scientific and technological innovation to support energy security and reliability. By partnering through working groups between Government and industry at the National, regional, State, and local levels, DOE facilitates enhanced cybersecurity preparedness.

As a recent example, DOE–OE and the National Association of Regulatory Utility Commissioners (NARUC) sponsored the third edition of a cybersecurity primer for regulatory utility commissioners. This document was published in January of this year and is publicly available on the NARUC Research Lab website, benefiting not only regulators, but State officials focused on the sector as well.

The updated cyber primer provides best practices, access to industry and National standards, sample questions, and easy reference materials for commissions in their engagements with utilities to ensure their systems are resilient to cyber threats.

We are continuing to work with the NARUC Research Lab to support regional trainings on cybersecurity throughout the year, with the goal of building commissioner and commission staff expertise on cybersecurity so they ensure cyber investments are both resilient and economically sound.

DOE also continues to work closely with our public and private partners to ensure that our response and recovery capabilities fully support and bolster the actions needed to help ensure the reliable delivery of energy. We continue to coordinate with industry through the SCCs to synchronize DOE and industry cyber incident response playbooks.

DOE–OE also engages directly with our public and private-sector stakeholders to help ensure we all are prepared and coordinated in the event of a cyber incident to the industry. Innovation and preparedness are vital to grid resilience. This past December, DOE and the National Association of State Energy Officials (NASEO) cohosted the Liberty Eclipse Exercise in Newport, Rhode Island, which focused on a hypothetical cyber incident that cascaded into the physical world, resulting in power outages and damage to oil and natural gas infrastructure. The event featured 96 participants from 13 States, and included representatives from State energy offices, emergency management departments, utility commissions, as well as Federal partners, such as FEMA, and private-sector utilities and petroleum companies.

In November, we are looking forward to participating in GridEx IV, which is the biennial exercise lead by the North American Electric Reliability Corporation (NERC) and is designed to simulate a cyber and physical attack on electric and other critical infrastructures across North America. Coordination with Federal partners and participation in preparedness activities enable DOE to identify gaps and develop capabilities to support cyber response as the SSA.

Leverage the expertise of DOE's National Labs to drive cybersecurity innovation

Beyond providing guidance and technical support to the energy sector, DOE–OE also supports an R&D portfolio designed to develop advanced tools and techniques to provide enhanced cyber protection for key energy systems. Intentional, malicious cyber threat challenges to our energy systems are on the rise in both number and sophistication. This evolution has profound impacts on the energy sector.

Cybersecurity for energy control and OT systems is much different than that of typical IT systems. Power systems must operate continuously with high reliability and availability. Upgrades and patches can be difficult and time-consuming, with components dispersed over wide geographic regions. Further, many assets are in publicly-accessible areas where they can be subject to physical tampering. Real-time operations are imperative and latency is unacceptable for many applications. Immediate emergency response capability is mandatory and active scanning of the network can be difficult.

The CEDS R&D program is designed to assist the energy sector asset owners by developing cybersecurity solutions for energy delivery systems through a focused research and development effort. DOE–OE co-funds projects with industry partners to make advances in cybersecurity capabilities for energy delivery systems. These research partnerships are helping to detect, prevent, and mitigate the consequences of a cyber-incident for our present and future energy delivery systems. Of course, our National Laboratories are critical partners in executing this work.

To select cybersecurity R&D projects, DOE constantly examines today's threat landscape and coordinates with partners, like DHS, to provide the most value to the energy sector while minimizing overlap with existing projects. For example, the Artificial Diversity and Defense Security (ADDSec) project will develop solutions to protect control system networks by constantly changing a network's virtual configuration, much like military communications systems that rapidly change frequencies to avoid interception and jamming. As a result, ADDSec can harden networks against the mapping and reconnaissance activities that are the typical precursors to a cyber attack.

Another project, the Collaborative Defense of Transmission and Distribution Protection and Control Devices against Cyber Attacks (CODEF), is designed to anticipate the impact a command will have on a control system environment. If the commands would result in damage to the system or other negative consequences, CODEF will have the ability to prevent their execution. This type of solution is especially intriguing as it can detect malicious activity regardless of the source, be it an insider threat or an external actor.

Since 2010, DOE–OE has invested more than $210 million in cybersecurity research, development, and demonstration projects that are led by industry, universities, and the National Laboratories. These investments have resulted in more than 35 new tools and technologies that are now being used to further advance the resilience of the Nation's energy delivery systems.

CONCLUSION

Threats continue to evolve, and DOE is working diligently to stay ahead of the curve. The solution is an ecosystem of resilience that works in partnership with local, State, and industry stakeholders to help provide the methods, strategies, and tools needed to help protect local communities through increased resilience and flexibility. To accomplish this, we must accelerate information sharing to inform better local investment decisions, encourage innovation and the use of best practices to help raise the energy sector's security maturity, and strengthen local incident response and recovery capabilities, especially through participation in training programs and preparedness exercises.

Building an ecosystem of resilience is—by definition—a shared endeavor, and keeping a focus on partnerships remains an imperative. DOE will continue its years of work coordinating with DHS and fostering vital energy sector relationships and investing in technologies to enhance security and resilience in order to support industry efforts to respond to, and recover quickly from all threats and hazards.

I appreciate the opportunity to appear before the subcommittee to discuss the cybersecurity of the energy sector. I would, however, be remiss if I did not take a moment to stress that the interdependent nature of our infrastructure requires that all sectors be constantly focused on improving their cybersecurity posture. Collaboration among DOE, DHS, and the rest of the Federal family is absolutely critical to ensuring that we remain both ahead of the curve and resilient to any potential cyber attack. DOE, as always, looks forward to our continued partnership to share best practices, collaborating where appropriate and possible, and helping to protect our civilian infrastructure from the Nation's cyber adversaries.

Mr. RATCLIFFE. Thanks, Ms. Hoffman.

I now recognize myself for 5 minutes of questions.

Ms. Manfra, I want to start with you. You mentioned Einstein and CDM in your testimony and the role that they play in securing Federal networks. So I want to give you an opportunity to provide some public clarity on the implementation of CDM specifically.

So can you give us some idea of how many departments and agencies have fully implemented CDM phase one and how many agency dashboards are up and running? Is the DHS dashboard up and running? Give us some perspective on that.

Ms. MANFRA. Yes, sir. Thank you for the question. We are in the process of deploying both phase one and phase two. Phase one being focused on hardware software asset management, sort-of identifying what is on the networks internal to the agencies, and phase two looking at who is on the network. So dealing with issues like access and identity management.

We can get back to you with the specific numbers of agency deployment. They are all in various stages of deployment. We have made it available to all agencies, but each individual agency is in different stages of deploying.

We are nearing 20 agencies that have an agency dashboard up and running. This month the Department of Homeland Security will be standing up the Federal dashboard, so that we will be receiving feeds from those agency dashboards.

That will then allow us to have more near-real-time understanding of what those sensors are identifying on those agency networks and allow us to better prioritize vulnerability management for our agencies.

Mr. RATCLIFFE. Terrific. Thanks. So one of the other points I wanted to cover today was, last week the GAO came out with a fairly critical report on the current state of Federal cybersecurity.

One of the most, would appear to be, at least, troubling aspects of that was a statistic that said only 7 of the 24 CFO Act agencies have programs with any functions considered effective per the NIST standards for cybersecurity control. So that doesn't sound very good.

I want to give either you, Mr. Krebs, or you, Ms. Manfra, the opportunity to, you know, as we talk about the cybersecurity posture of the dot.gov reconcile that with that GAO report.

Ms. MANFRA. Sir, I think that we have learned a lot over the years about agency capacity to manage cybersecurity risks and the resources they have to do so. I can say that agencies have prioritized the management of their cyber risk at their highest level across the Government.

What we have learned in both the deployment of CDM, our engagement and partnership with OMB in measuring agencies is that there remain some significant gaps.

We have built over the last couple years and are continuing to build a technical assistance capabilities, things like design and engineering, architecture reviews, helping agencies getting much more in-depth insight into their networks and providing them with a greater level of assistance, both engineering and on the governance side to help them address their often very complicated networks with the limited resources we have.

But we do see a lot of potential for CDM in the ability to deliver tools at a lower cost across agencies and this is the first time that many agencies have had access to this level of automated data to understand what is on their network.

So we see a lot of potential for this, but for many agencies there is a lot of capability that has to be built. We are continuing to take advantage of things like shared service, more capability from DHS to deploy to agencies who need it most.

Mr. RATCLIFFE. So your comment about shared services and resources, I want to follow up on that a bit because I think it is important to look where we are but also look to where we are going.

So looking forward a bit, how do you see DHS's Federal network protection tools evolving past, say, signature-based threat detection tools and particularly where my conversations with the administration and the cybersecurity advisors to the President, really putting an emphasis on cloud computing and shared I.T. services and resources?

So I guess, in a sense, what is Einstein future generations—Einstein 10.0 look like?

Ms. MANFRA. Well, sir, I am not exactly sure what Einstein 10.0 will look like yet, but I can tell you where we are looking to evolve. As agencies, and the President's key initiative around modernizing our I.T. and that is not just the technology.

There are large challenges with legacy technology, but we also need to modernize the way we govern and procure I.T. services within the Government. As we do that we are working very closely to modernize our security processes.

So as we take advantage of things like cloud services we ensure that we are modernizing our security approach, but also not losing the insight that we have into traffic, either traversing internal networks or in and out of agency networks.

Importantly we have learned on CDM some key lessons from the first phases of deployment. We now have a new contract vehicle in place that will enable the deployment of cloud and mobile security technologies in addition to the on-premise sensing capability that we have right now.

So we are evolving. We are building on what industry is learning from behavioral-based detection methods, and we have had some successful pilots. We look forward to continuing to build that capability.

Mr. RATCLIFFE. Terrific. Thanks very much. My time has expired.

The Chair now recognizes Mr. Richmond for his questions.

Mr. RICHMOND. Ms. Manfra or Mr. Krebs, either one, you all know that I authored legislation that called for a Department-wide cybersecurity strategy within DHS. That strategy and report was due in March. We still don't have it.

So what is the status of it; if you are running into problems in getting it done, what are those problems? How can we help?

Mr. KREBS. Sir, thank you for the question. The Office of Policy has the pen, so to speak, for drafting the Department cybersecurity strategy. It rolls in components across the Department, between the Secret Service, ICE, Homeland Security Investigations, the U.S. Coast Guard, Transportation and Security Administration, as well as NPPD.

So while we don't necessarily lead the development of that strategy because it is a Department-wide strategy, we are a significant player.

Now, to speak to the status of the strategy itself, my understanding of where it sits is influenced by the President's Executive Order 13800 that was released back earlier in the spring.

Now that report puts DHS at the front or in the lead for almost all of the reports, particularly in the first two and the fourth work stream, Federal networks' critical infrastructure and cyber work force. So while those reports and assessments are under way, they are anticipated to have significant impacts on some of the priorities perhaps of the Department, including NPPD.

So I believe the decision on finalizing the strategy has been to let's get through the cybersecurity assessments related to the E.O., as well as the administration's anticipated National security strategy and National cybersecurity strategy that are expected in the next several months.

Then, when we have a broader understanding of where the Department is going, that will then feed into the cybersecurity strategy.

That said, rolling it all back to the requirement in the NDAA—that you offered, it still is a priority to finalize that report. That said, as a Department, we are moving forward with a number of our priorities.

I do want to touch on a couple things you mentioned early. As the senior official performing the duties of the under secretary, while we do not have a permanent under secretary for NPPD, I have been authorized and given the very clear direction by acting Secretary Duke to move out and execute every aspect of NPPD.

So while we do not have a permanent under secretary right now, I have all authority that I believe I need to execute the Department's mission within NPPD.

Mr. RICHMOND. With regards to a strategy, and we talk about in terms of report, let me just take that aside.

Mr. KREBS. Yes, sir.

Mr. RICHMOND. Do we have a Department-wide strategy with how we deal with cybersecurity and our needs and challenges that we are going to continue to face in the near future?

Mr. KREBS. Sir, my understanding is that there is a Department-wide cybersecurity strategy in draft form, yes, sir.

Mr. RICHMOND. So and again with—I don't want to get into the weeds. I am just saying are you all operating with some comprehensive strategy——

Mr. KREBS. Yes.

Mr. RICHMOND [continuing]. On a day-to-day basis to protect the cybersecurity?

Mr. KREBS. I understand, yes, sir. So going back to my opening remarks, I indicated that NPPD is in the lead for ensuring the Nation's critical infrastructure, both cybersecurity and physical threats, and under that are three goals.

I mentioned the top goal, which is securing our Federal networks and facilities. For me and with Assistant Secretary Manfra, that is at the very top of our minds every, single day.

The second piece is identifying and mitigating systemic risk across the infrastructure, the Nation's infrastructure. When I think about that, I am thinking about the Section 9, critical infrastructure at greatest risk, but I am also putting election infrastructure in there.

As I mentioned in my opening comments, that, for me, is the No. 1 priority for NPPD from a critical infrastructure perspective. We cannot fail there.

Third and finally, is enabling and incentivizing better security practices across the broader critical infrastructure community to include State, local, small, and medium-sized businesses.

Mr. RICHMOND. Ms. Hoffman, there has been a great deal of concern among National security experts that Russia's goal in disrupting the Ukraine's power supply in 2015 and 2016 was to test its capabilities in preparation for a large attack on the United States.

Last month we learned that Russia may have been responsible for Dragonfly 2.0, which exploited and targeted some of our energy sector. How is the energy sector responding and what is their capabilities to prevent a wide-spread attack?

With that, I yield back.

Ms. HOFFMAN. Thank you, Congressman, for the question. The Ukraine attack was very much an eye-opening event for the energy sector. The energy sector, specifically the electric sector, got very organized in recognizing that we had to continue to step up our continuous monitoring capabilities, our ability to detect behavior on the system, but also building inherent protections as we develop new technologies.

Recognize that the core of anything is protecting against spearfishing and passwords and credentials and that starting to really go after where do we need to be with respect to preventing an attack from occurring on the system. So we have been working very actively with the electric sector to build some tools and capabilities and for protections of their system.

Mr. RATCLIFFE. The Chair now recognizes the gentleman from New York, Mr. Donovan for 5 minutes.

Mr. DONOVAN. Thank you, Mr. Chairman. I would just like to ask one question of all of you. In 2015, Congress passed the Cybersecurity Act of 2015. In 2017, the committee passed the Cyber and Infrastructure Security Agency Act, and the President also issued an Executive Order back in May to strengthen our abilities.

What do you guys need? What can Congress do to help you protect our Nation, our Federal agencies, our private entities, as Mr. Richmond said, our energy industries? What do you guys need from us to help you protect our Nation better than we are able to do now?

Mr. KREBS. Sir, thank you for the question. The very first thing I would start with is, as you mentioned, the Cybersecurity and Infrastructure Security Agency Act in 2017. Passing out of the full committee was a significant step forward. What we need, as I mentioned in my opening comments, is quick action by the full House and the Senate. Let me give you a little anecdote about why that is important. That bill will give us three things.

One, it will allow us to introduce some operational efficiencies, looking at common infrastructure across the organization, push them together so that we are more streamlined in how we engage and deliver services from a customer service orientation.

Second, it will help with our branding and clarify roles and responsibilities not just within NPPD, but more importantly, with our Federal partners, State and local partners, and the private sector. I want to come back to that in just a second.

Finally what that is going to do is give us the ability to attract talent. We have talked a little bit about work force, we talked about hiring, and we talked about partnership. But on that clarity of roles and responsibilities, let me talk about that for just a second.

I have been down to Puerto Rico twice in the last week. I was there last Monday with Administrator Long and the President's Homeland Security Advisor Tom Bossert, and then I was there last Friday with Acting Secretary Duke.

On Friday, meeting with Acting Secretary Duke, Governor Rossello and his key staff, we were discussing a number of the critical infrastructure challenges in Puerto Rico.

When it came around to me, I talked about communications infrastructures. As you all know, the National Communication Center resides within the Office of Cybersecurity and Communication, Assistant Secretary Manfra's organization.

Now when we talked about the status of things, what I was talking about was how we are assisting the communications carriers, whether it is AT&T, Sprint, Claro, T-Mobile, Verizon, helping them get back in, prioritize deliveries of temporary capabilities, this cell on wheels, cell on light trucks, things like that, to helping temporarily pop up the communications coverage, but at the same time helping them get resources in for cell towers.

Now as I briefed out where we were on helping those companies get resources back in, I introduced myself as the senior official performing the duties of the under secretary for the National Protection and Programs Directorate. Now, try repeating that back. It is not easy.

So someone that has never heard that before, immediately went on to a press interview and alongside the TSA administrator, vice commandant of the Coast Guard, the secretary of Homeland Security, the FEMA regional administrator, she said, "We at FEMA, TSA, Coast Guard, and the COMS guy." She didn't know how to describe me.

When I am out engaging my stakeholders, they don't understand the mission I deliver. I need help in clarifying that and providing very front, up front clear what I do and what my team delivers. That is a significant advancement. So any help I can get there, please, help me out.

But more broadly though, in terms of additional authorities and clarification of authorities, we are in the process of running that kind of stocktaking of where the Department sits in cybersecurity.

Department of Energy in the FAST Act got significant authorities that could come to bear in the event of a grid incident. DHS has authorities in terms of incident response, information sharing. Thank you for those authorities.

Going forward, we are not quite sure just yet what we need, but I am going to tell you this. The cybersecurity threat is not going away. Our adversaries are getting better, they are getting faster, they are getting more agile.

We need to be resourced, we need to be staffed, we need to be positioned to respond to that, because I also know one more thing. We are not going to use less technology going forward.

As you indicated earlier, we are going to the cloud. We are going to shared services. We are going to be relying upon these cross-cutting technology capabilities in the information technology sector. We need to ensure that from a digital defense perspective, we have what we need.

So we welcome that conversation, and you can believe that you will see me again and we are going to be talking about that.

Mr. DONOVAN. Ms. Manfra, I have 2 seconds left in my—would you contribute, please?

Ms. MANFRA. Yes, sir. Very briefly just to complement what Chris talked about, we are working within the Federal Government to understand what is the full breadth of our authorities? How can we lean into the existing authorities that they have to deploy more capability?

With the critical infrastructure sectors, we are working to understand now that we have identified these most critical assets at greatest risk, are there legal and operational and policy hurdles that we need to address in order to ensure that we have appropriate prevention and response and recovery capabilities in place? So we look forward to working with you as we conclude these analyses.

Mr. DONOVAN. Please don't wait until another hearing. Let us know how we can help you.

Ms. MANFRA. Absolutely, sir.

Mr. DONOVAN. Mr. Chairman, I yield back the time I don't have left.

Mr. RATCLIFFE. Thank the gentleman.

The Chair recognizes the gentleman from Mississippi, Mr. Thompson.

Mr. THOMPSON. Thank you, Mr. Chairman. The last two speakers have talked about being resourced and staffed from an agency standpoint. Last March we held a hearing talking about staffing at the Department. Can you give us the number of unfilled positions in the cyber division right now?

Ms. MANFRA. Sir, we are currently staffed at 76 percent of our fully-funded billet.

Mr. THOMPSON. So we are 24 percent under. Can you tell us why we are understaffed at this point?

Ms. MANFRA. Yes, sir. There are a variety of reasons. The first, largely thanks to the work in this committee and our appropriations staff in Congress in building the billets that are allocated to my organization, we have grown significantly. We have worked very hard to build according to that growth in billets, but we have had some challenges.

We have worked with our management, colleagues, and our human capital colleagues to identify areas where we can reduce the time to hire. I can say that looking at the statistics from fiscal year 2016 hiring to fiscal year 2017 hiring, we have been able to reduce the time to hire by 10 percent.

Many of these requirements have to do with security clearances. It does take a long time to process people through that security clearance process, but we have made significant progress. We are continuing to work with our security office to identify ways that we can continue to shorten that.

We are also diversifying our recruitment path, looking at the scholarship for service. The CyberCorps program has been a great pipeline for us to bring to—after we, the Government has funded scholarships, bringing these individuals in as interns and then hiring them full-time.

They are already fully qualified for our direct hire authority. Looking at other programs such as Pathways, Presidential Management Fellows and other recent graduate programs. We are also looking at partnerships with industry where they can——

Mr. THOMPSON. I don't mean to cut you off, but——

Ms. MANFRA. Yes, sir.

Mr. THOMPSON [continuing]. So is the problem we have too many programs to attach people to? Or I am just trying to find out why when we give you the authority to hire, why we have not been able to come closer to whatever that authority is. Is there something——

Ms. MANFRA. I see, sir.

Mr. THOMPSON [continuing]. We need to do to get you to that point?

Ms. MANFRA. Sir, I separate the authority that we were given by Congress to build an accepted service program. What I was referring to was I did not believe a couple of years ago we were fully leveraging the authorities we already had and the programs that we already had to bring people in and tightening the time line that it takes to bring people on.

The accepted service program is led by our chief human capital officer, who I know this is a high priority for her. We did not probably appropriately expedite the development of that program 4 years ago. We have now done so.

My understanding is that we will now be able to hire against that program beginning in fiscal year 2019, but there is a regulatory process that we do have to undergo as a part of that.

Mr. THOMPSON. Just for the sake of the committee, can you provide us with a time line between when somebody who is considered for employment and when that is completed? Is it—just get back to us.

Ms. MANFRA. Yes, sir.

Mr. THOMPSON. Was it 3 months, 6 months, a year? I think that would be instructive for us so we can kind of see if there are some bottlenecks involved.

Ms. MANFRA. Yes, sir.

Mr. THOMPSON. The reason I say that, Mr. Chairman, I mean, all of us are constantly bombarded by people looking for employment opportunities. If we have potential opportunities here, is it something we are not doing? Are we not going out recruiting in a broader view or just what? But we just need to——

Ms. MANFRA. Sure.

Mr. THOMPSON [continuing]. Kind-of figure something out.

Ms. MANFRA. Right. If I could, sir, just clarify that the 76 percent is just indicating people that are on-board right now. If you include the people that are in the full pipeline, that brings us about to 85 percent.

So for us, we are averaging about 224 days to hire. That sounds long, but that is to include a Top Secret SCI clearance process, which is actually fairly for the benchmark of the rest of the Government, we are actually doing quite well.

We want to continue to work with you sir, though. We will come back with you.

Mr. THOMPSON. Just, please get back——

Ms. MANFRA. Yes, sir.

Mr. THOMPSON [continuing]. With us.

Mr. Krebs we have a Congressional Task Force on Election Security, and we may request of the Department to provide us a Classified briefing around this issue. We have been told that it has to be bipartisan, that you can't just brief Democrats. Are you aware of that?

Mr. KREBS. Sir, I am not aware of any existing policy, but let me say this. I share your concern on election infrastructure. I think I have made that clear today, and I want to say it directly to you as well, that it is my top priority at the Department.

Again, if we can't do this right, if we can't dedicate every single asset we have to assisting our State and local partners, then, frankly, you know, I am not sure what we are doing day-to-day.

So in terms of what we have done in terms of engagements, we are prioritizing delivery of those briefings, information sharing to our State and local partners. We are doing it in a bipartisan manner because my opinion is that this does transcend party lines, and we should be doing this, all pull in the same direction.

So going forward, I would encourage any additional briefings. We have provided a series of bipartisan briefings to the House Homeland Security Committee, both Classified and Unclassified. The real crux of this issue, the underpinning issue here, is a trusted relationship.

Now, did we have some—yes, sir——

Mr. THOMPSON. I appreciate it, but we have established a working group within the Democrats on the committee, and we are just trying to get a briefing. So I think it is nice to say I don't want to brief you because there are no Republicans, but we are Members of Congress. All we are trying to do is get access to the information.

If your interest is there, I am convinced that you will provide it. That is the spirit in which the request was made. So we will make it again.

Mr. KREBS. Yes, sir.

Mr. THOMPSON. I look forward to you coming back. Just bring us what information you have as Members of Congress, and that is all we ask.

Mr. KREBS. Thank you.

Mr. THOMPSON. I yield back, Mr. Chairman.

Mr. RATCLIFFE. Thank the Ranking Member.

The Chair now recognizes the gentleman from Virginia, Mr. Garrett.

Mr. GARRETT. Hit my talk button. My voice sounds better with the microphone on. But I want to piggyback on what my friend and colleague, Ranking Member Thompson said, and suggest that I would agree with you that election infrastructure, cybersecurity as it relates to partnering with States whose responsibility it is to overseeing and conduct elections is a priority that crosses and transcends the aisle.

I would ask that any briefing that you give to Democrat Members you also perhaps invite me to or give the exact same briefing to Republican Members, which I think is inconsiderate of your time given that that would be a great redundancy.

But I can't fathom why one party should be briefed on cybersecurity as it relates to our elections in the absence of another in the United States of America.

So if you do, in fact, and I hope you will, respond to the Ranking Member's request to brief on electoral security as it relates to cyber issues, please invite me, because I can't fathom that one party has a monopoly on hoping that we can have free and fair and trustworthy elections.

I am sure that my colleague didn't mean it that way, but I just want to be very clear in suggesting that that should not be a partisan issue and that perhaps maybe people from both parties should be invited. Or we can just make you give the same briefing twice which, again, I think is inconsiderate and shortsighted.

Having said that, transitioning to what we know as it relates to malicious Russian cyber activity, specifically with relation to Estonia and the Ukraine, based on my understanding, the bulk of the platforms used to infiltrate infrastructure—I say, platforms—malware, it would appear, based on my ability to speak in this forum, were off the shelf, if you will, Kill This, or example, Black Energy were known entities that were discovered as it relates to these attacks as part of a coordinated attack. How well do we stay ahead or try to stay on-line with it?

I understand that it is a moving target, the malware that might be implemented because to the extent that there is any hope, and again, I understand the format that we are in might limit the conversation that we have, a lot of the malicious activity to this point conducted we presume and data would indicate by the Russians has used off-the-shelf technology.

So I guess the question there is how quickly can we pick up on the advancements in malware and then sort-of inculcate them into our preventative measures? That is wide open to whichever one of you wonderful folks would like to address it.

Mr. KREBS. Thank you, sir. So if I may, I will start and provide a bit of a broader approach and then defer to my expert colleague from the Department of Energy on anything specific to the grid and electricity.

Mr. GARRETT. I am subject to a time limit, so, I apologize but——

Mr. KREBS. So I will do this quickly.

Mr. GARRETT. Yes, sir.

Mr. KREBS. Generally speaking when we talk—we have already talked about advanced persistent threat here. When we think about threats, it is not necessarily generally speaking advanced. It is just persistent.

Companies are—organizations are still not doing the basic blocking and tackling. When you think about WannaCry, when you think about NotPetya, some of those exploitations were based on open, known vulnerabilities. They just weren't patched.

So the concept of a zero-day exploit, while it is out there, it is not actually the primary exploit that we tend to see in the wild.

Mr. GARRETT. Sorry to interrupt you. I am a big fan of limited government, but in this arena, because the entire Nation hangs in the balance, not just our elections but everything as it relates to our grid, might it not be effective to hit the particular power providers where it counts?

That is essentially make it cost something, perhaps metaphorically and literally, for entities that don't patch those open known threats. That is something that would be within the purview of the Government, right? You will be up to date on X, Y, and Z or it will cost you. Would that be something that has been explored?

Mr. KREBS. So my colleague, Jeanette Manfra, can speak to the Government piece. Then——

Ms. MANFRA. OK, just very briefly——

Mr. GARRETT. Again, I am not trying to—you guys are great, I just, 5 minutes.

Ms. MANFRA. No problem. So very briefly, the first binding operational directive we issued for Federal agencies was reducing the time to patch critical vulnerabilities, as you said, 30 days.

We have actually seen a complete cultural change as a result of that. We are now seeing the Government highly prioritizing patching those critical vulnerabilities. So I just wanted to throw that out there.

Mr. GARRETT. So there is a carrot and a stick, right?

Ms. MANFRA. Correct, sir.

Mr. GARRETT. I am guessing the stick, but the carrots—I would rather the carrot. But I am glad to hear you say you are addressing that. Again Mr. Hoffman, I don't mean to cut you short. I have got 15 seconds.

I wanna speak to the nature of NERC and whether or not the fact that it is a semiprivate autonomous pseudo-entity compromises intelligence tactics, techniques, procedures, et cetera.

Ms. HOFFMAN. So I don't think NERC as an organization compromises any sort of intelligence. It does have the information-sharing analysis center, which is our mechanism for sharing information to the sector writ large. It also has capabilities to compel and look at the industry to respond so we can get the information we need.

Mr. GARRETT. Thank you all, and I apologize for going briefly over.

Mr. RATCLIFFE. Thank the gentleman.

The Chair recognizes my friend from Rhode Island, Congressman Langevin.

Mr. LANGEVIN. Thank you, Mr. Chairman. I want to thank our witnesses for your testimony here.

Before I go into my questions, I just wanted to mention publicly and particularly to Mr. Garrett, so I am a member of the elections task force that certain Democrats have put together on how to go forward and improving election security.

I would say to my colleague that there was an initial effort in outreach to Republicans to make this a bipartisan effort, which was not accepted. It was not—we didn't find anyone that was receptive. But I would say this. The task force meetings are open to the public. My colleague Mr. Garrett is welcome to participate fully with that.

With respect to the Ranking Member's question on the Classified briefing both on Russian interference in our elections and how we are better securing our election systems, that is whether it was a Democrats only or Democrats and Republicans, I would prefer it as a Democrat and Republican briefing.

But however we get the briefing, unless I am misunderstanding what the Ranking Member was asking, we just want the briefing. So we have asked that you provide that to us.

Mr. KREBS. Yes, sir. Thank you. I do believe we have provided a Classified briefing in the past and welcome the full committee briefing and the subcommittee briefing on that as well. Yes, sir.

Mr. LANGEVIN. So the other thing I wanted to mention that, Mr. Krebs, I appreciate your comments, that you have all the authorities in your acting role to do the job necessary in cyber. But I would reiterate that it is vitally important that we get key people appointed and in place permanently.

I respect the work that you are doing and your team, but we need permanent people in place. It both inspires confidence and clarity to what the mission is.

So let me get into my questions very quickly. I am gonna try to go through them. For the ones you can't answer fully because of time constraints, I would request a follow-up in writing.

So on September 13, DHS issued a binding operational directive, 1701, which directed Federal Executive branch departments and agencies to remove Kaspersky products from their systems within the next 90 days.

In doing so, DHS for the first time issued a public statement to coincide with the establishment of the directive and which I would like to commend the Department for this added transparency. I thought that was important.

My question is: What analysis led to the removal of Kaspersky from Federal networks? This is the case—I understand that this answer may be Classified, in which case I would request it that you and your team provide briefing to Members on the deliberations behind it. I think that is something vitally important that this committee, both sides of the aisle, understand what went into that.

Next Mr. Krebs, the SEC was breached in late 2016. We now know that the attackers had access to corporate filings prior to their public release. The announcement of this breach was made nearly a year after it was first discovered.

My question was: When was DHS informed of the breach? What was DHS's involvement in detecting, responding, and recovering from this attack?

Finally, how could DHS improve its integration with Federal agencies to ensure these types of attacks are detected and notified quicker in the future?

Mr. KREBS. Thank you, Congressman Langevin. Let me briefly touch on the Kaspersky piece, and then I will kick it over to Assistant Secretary Manfra. So on Kaspersky, that determination was based on the totality of evidence including by, on the most part open-source information.

In terms of a Classified briefing, I believe we are on the schedule for some point in the next month or so with the full committee, the monthly intel briefing. So with that, if I may, I would like to turn it over to Assistant Secretary Manfra.

Mr. LANGEVIN. Thank you. I would appreciate it. Thank you.

Ms. MANFRA. Sir, welcome to support a briefing on Kaspersky. As far as the SEC, we are also happy to come in and have a more fulsome conversation with you about that. They did notify us last year on November 4 of an issue.

It was, at the time, the extent of the issue was not well-understood and given the time limits here, I think it might be more useful if we sat down with you and other staff members as appropriate to walk through specific details.

Mr. LANGEVIN. OK. What do you think—what was the DHS involvement, though, in detecting and responding to the recovery though?

Ms. MANFRA. Sir, we have very limited involvement with the SEC. They did not request our follow-on assistance for a response.

Mr. LANGEVIN. OK. On the issue of how they can work better in the future?

Ms. MANFRA. Sir, in addition to this incident, as well as several others, we are reviewing our procedures to ensure that it is clear that when an incident happens, what role that the Department needs to play in a response, not just at the request of an agency.

That if we are looking at specific critical services and functions then the Department needs to have a more active role in that response, regardless of whether the agency requests it.

Mr. LANGEVIN. Thank you. In August, Congressman Will Hurd and I traveled to DefCon as a bipartisan trip to that security conference. I think we both were impressed by the willingness of security researchers to report vulnerabilities in order to improve overall internet security.

What efforts has the Department made to establish a vulnerability reporting process for DHS sites and software? Again, one of the things that I found with sort-of the Pentagon's bug bounty program was very helpful in identifying security vulnerabilities and getting the attention of the right individuals to close those vulnerabilities.

In talking to security researchers, one of the things that impressed me the most is that they just want to make the internet work better. But they wanna know that when they find a vulnerability, there is a path forward that they can report it and that someone is actually gonna do something about it and they are actually gonna be heard.

So what progress has DHS made in this respect?

Ms. MANFRA. Sir, we actually have a very long-standing program on both operational technology vulnerabilities, so industrial control systems as well as enterprise technologies.

We have been working with security researchers in both communities for years to provide them a space for them to identify that vulnerability and also to advocate with the owner of that software for a patch. Much of the alerts that we issue are the result of collaboration with security researchers.

We also have our own organization within my group that conducts penetration testing and risk and vulnerabilities assessments across the Government to include DHS networks.

So while bug bounty programs can be useful, we need to ensure that they are supplemented with a broader risk and vulnerability analysis and testing that my organization does to ensure organizations are appropriately prioritizing what they are addressing.

Mr. LANGEVIN. OK. What about DHS's specifically-owned systems?

Ms. MANFRA. My organization also supports penetration testing and vulnerability assessments within the DHS, particularly the high-value assets that DHS owns.

But I do know that our leadership and the management is interested in learning from what the Department of Defense has done in their bug bounty program and how that might apply to DHS. So we are continuing to work through how that might be applied for our organization.

Mr. LANGEVIN. Mr. Chairman, I had one more on election security. Can I ask that? Thank you.

So I know we have touched on this a bit, but for the record I really wanted to dive a little deeper into this. So I am very interested, obviously, in ensuring that State and local election officials have access to resources from DHS to protect the vital systems that represent the cornerstone of our democracy.

So can you further describe how DHS is working with election officials to protect networks? Do you believe that DHS's response to the unprecedented appearance in our elections last year really has been sufficient?

Finally, how can we improve the relationship and access to resources? Are there additional funds or resources that the Department needs in this respect?

Mr. KREBS. So thank you for those questions. Let me start at the end with your improving relationships. While I was not at the Department last summer as this all manifested, I can speak to generally the relationships with State election officials.

That was not an existing relationship between the Department of Homeland Security in the State and locals. However, we do have strong relationships, of course, with the Homeland Security advisors and the chief information officers and chief information security officers.

But to square the circle on this specific threat, we need to develop partnerships that are, you know, three or four legs on the stool within each specific State. Each State is going to be a little bit different in terms of how, you know, who they designate as the chief election official, as well as you roll in the vendors of technology.

So in terms of how to improve relationships, it is gonna take a lot of effort and a little bit of time. Those are things that we are working on right now. We don't have much time, but we are dedicating resources.

In fact, just this morning I sent out a notice across my organization, NPPD, reflecting some changes we made organizationally last week by establishing an election task force.

Previously, the election infrastructure piece had been held within the Office of Infrastructure Protection as a program.

Again, matching my words with our execution, we are elevating it as a task force, bringing components or pieces from across the DHS components, including the Office of Intelligence Analysis and resourcing it appropriately.

This is speaking to a lot of resources. We are pulling the resources together in recognition that we don't have a lot of time, given there are three elections this year.

Mr. LANGEVIN. The number of FTEs and money that is it actually committed to this?

Mr. KREBS. I don't have the FTEs on hand right now. But I can get back to you on that one. I believe Miss Manfra has them.

Mr. LANGEVIN. The funds as well, specifically?

Ms. MANFRA. Yes. If I could just make one additional point on the resources, Ranking Member Richmond noted that his understanding was that there was a 9-month wait for risk and vulnerability assessments. I don't know whether that is the exact current number.

But that speaks to the high demand that we are experiencing for our assessment services. That is everything from penetration testing to the cyber hygiene scans that multiple States and localities have participated and continue to participate in, as well as these more in-depth risk and vulnerability assessments.

We are growing that program. We are diverting resources. We are building infrastructure so that we can more scale that. But these are services that we are providing not just to Federal agencies, but also to State and local governments, as well as critical infrastructure. We are experiencing much more demand for those services, and we are continuing to look for ways to scale that capability.

Mr. LANGEVIN. Thank you. Thank you for your answers. Again, if there are follow-ups that you can provide to give us in writing or in briefings, I appreciate that.

Mr. Chairman, thank you for your indulgence.

Mr. RATCLIFFE. You are welcome. The gentleman yields back.

I wanna thank all three of our witnesses today for your valuable and insightful testimony. I thank all the Members for their questions today. The Members of the committee do have some additional questions for witnesses, and we will ask you to respond to those in writing.

Pursuant to committee rule VII(D), the hearing record will be held open for a period of 10 days. Without objection, the subcommittee stands adjourned.

[Whereupon, at 11:28 a.m., the subcommittee was adjourned.]

APPENDIX

Questions From Chairman Michael T. McCaul for Christopher Krebs

Question 1a. What is DHS doing and what more is planned for the future to assist in and refine the process of providing clearances for those in the private sector?

Answer. Response was not received at the time of publication.

Question 1b. Has there been talk of allowing for more clearances if the private sector were willing to pay for each additional clearance for individuals who qualify via the current standards?

Answer. Response was not received at the time of publication.

Question 1c. There also seem to be issues in clearing secure facilities. Is the Department making the appropriate relevant information available to the private sector on what the qualifications are for obtaining a cleared facility?

Answer. Response was not received at the time of publication.

Question 2a. When it comes to information sharing, DHS has a variety of programs from CISCP, to AIS, to the individual agreements with the Information Sharing and Analysis Centers. How is DHS incorporating stakeholder feedback to understand what information is most useful and actionable for companies?

Answer. Response was not received at the time of publication.

Question 2b. What are the greatest challenges faced by the information-sharing programs?

Answer. Response was not received at the time of publication.

Question 2c. Has there been any operational change to the amount, type, or context around the cyber threat information shared to address these challenges?

Answer. Response was not received at the time of publication.

Question 3. The protection of Federal networks was a large element of the President's cyber Executive Order (EO). As DHS is currently implementing the Continuous Diagnostics and Mitigation (CDM) program to protect Federal networks, what is the role CDM in executing the EO?

Answer. Response was not received at the time of publication.

Questions From Chairman John Ratcliffe for Christopher Krebs

Question 1. In 2014, DHS was provided authority to establish excepted service positions relating to cybersecurity; what is the time line for implementation and operationalization of this authority?

Answer. Response was not received at the time of publication.

Question 2a. In 2015, Congress passed important legislation authorizing the Automated Indicator Sharing program, or AIS. Is AIS currently meeting the benchmarks that have been had laid out for the program?

Answer. Response was not received at the time of publication.

Question 2b. What are the reasons for the successes DHS has had with AIS and what are some impediments that the program is currently facing?

Answer. Response was not received at the time of publication.

Question 2c. What are the latest benchmarks that DHS has set for AIS and what can we in Congress do to support these efforts?

Answer. Response was not received at the time of publication.

Question 3. There seems to be a consensus that in order to keep pace with the threats our networks face, collaboration between the public and private sector will need to be strengthened. How do you see engagement and collaboration with the private sector changing?

Answer. Response was not received at the time of publication.

Question 4. As part of the cyber Executive Order, the DHS Secretary will be reviewing the capabilities and resources that can be and currently are being offered to designated companies within the most critical of critical infrastructure sectors (Section 9 companies). Please provide a general overview of what is currently offered. Do you expect any additional capabilities to be developed or implemented by DHS for companies designated as "Section 9" in response to this review?

Answer. Response was not received at the time of publication.

QUESTIONS FROM CHAIRMAN MICHAEL T. MCCAUL FOR JEANETTE MANFRA

Question 1a. What is DHS doing and what more is planned for the future to assist in and refine the process of providing clearances for those in the private sector?

Answer. Response was not received at the time of publication.

Question 1b. Has there been talk of allowing for more clearances if the private sector were willing to pay for each additional clearance for individuals who qualify via the current standards?

Answer. Response was not received at the time of publication.

Question 1c. There also seem to be issues in clearing secure facilities. Is the Department making the appropriate relevant information available to the private sector on what the qualifications are for obtaining a cleared facility?

Answer. Response was not received at the time of publication.

Question 2a. When it comes to information sharing, DHS has a variety of programs from CISCP, to AIS, to the individual agreements with the Information Sharing and Analysis Centers. How is DHS incorporating stakeholder feedback to understand what information is most useful and actionable for companies?

Answer. Response was not received at the time of publication.

Question 2b. What are the greatest challenges faced by the information-sharing programs?

Answer. Response was not received at the time of publication.

Question 2c. Has there been any operational change to the amount, type, or context around the cyber threat information shared to address these challenges?

Answer. Response was not received at the time of publication.

Question 3. The protection of Federal networks was a large element of the President's cyber Executive Order (EO). As DHS is currently implementing the Continuous Diagnostics and Mitigation (CDM) program to protect Federal networks, what is the role CDM in executing the EO?

Answer. Response was not received at the time of publication.

QUESTIONS FROM CHAIRMAN JOHN RATCLIFFE FOR JEANETTE MANFRA

Question 1. In 2014, DHS was provided authority to establish excepted service positions relating to cybersecurity; what is the time line for implementation and operationalization of this authority?

Answer. Response was not received at the time of publication.

Question 2a. In 2015, Congress passed important legislation authorizing the Automated Indicator Sharing program, or AIS. Is AIS currently meeting the benchmarks that have been had laid out for the program?

Answer. Response was not received at the time of publication.

Question 2b. What are the reasons for the successes DHS has had with AIS and what are some impediments that the program is currently facing?

Answer. Response was not received at the time of publication.

Question 2c. What are the latest benchmarks that DHS has set for AIS and what can we in Congress do to support these efforts?

Answer. Response was not received at the time of publication.

Question 3. There seems to be a consensus that in order to keep pace with the threats our networks face collaboration between the public and private sector will need to be strengthened. How do you see engagement and collaboration with the private sector changing?

Answer. Response was not received at the time of publication.

Question 4. As part of the cyber Executive Order, the DHS Secretary will be reviewing the capabilities and resources that can be and currently are being offered to designated companies within the most critical of critical infrastructure sectors (Section 9 companies). Please provide a general overview of what is currently offered. Do you expect any additional capabilities to be developed or implemented by DHS for companies designated as "Section 9" in response to this review?

Answer. Response was not received at the time of publication.

○