MAXIMIZING THE VALUE OF CYBER THREAT INFORMATION SHARING

HEARING

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY AND INFRASTRUCTURE PROTECTION

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTEENTH CONGRESS

FIRST SESSION

NOVEMBER 15, 2017

Serial No. 115–39

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

29–472 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
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
VACANCY

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

The Honorable John Ratcliffe, a Representative in Congress From the State of Texas, and Chairman, Subcommittee on Cybersecurity and Infrastructure Protection:
Oral Statement 1
Prepared Statement 3
The Honorable James R. Langevin, a Representative in Congress From the State of Rhode Island:
Oral Statement 4
Prepared Statement 7
The Honorable Bennie G. Thompson, a Representative in Congress From the State of Mississippi, and Ranking Member, Committee on Homeland Security:
Prepared Statement 8
The Honorable Sheila Jackson Lee, a Representative in Congress From the State of Texas:
Prepared Statement 9

WITNESSES

Mr. Robert K. Knake, Whitney Shepardson Senior Fellow, Council on Foreign Relations, On Behalf of The Global Resilience Institute:
Oral Statement 11
Prepared Statement 12
Ms. Ann Barron-Dicamillo, Vice President, Cyber Intel & Incident Response, American Express:
Oral Statement 18
Prepared Statement 20
Ms. Patricia Cagliostro, Federal Solutions Architect Manager, Anomali:
Oral Statement 23
Prepared Statement 24
Mr. Robert H. Mayer, Senior Vice President for Cybersecurity, USTelecom Association:
Oral Statement 27
Prepared Statement 29

FOR THE RECORD

The Honorable James R. Langevin, a Representative in Congress From the State of Rhode Island:
Letter 6

APPENDIX

Questions From Congressman James R. Langevin for Robert K. Knake 47
Questions From Honorable James R. Langevin for Ann Barron-Dicamillo 48
Question From Honorable James R. Langevin for Patricia Cagliostro 49
Questions From Honorable James R. Langevin for Robert H. Mayer 50

MAXIMIZING THE VALUE OF CYBER THREAT INFORMATION SHARING

Wednesday, November 15, 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 2:47 p.m., in room HVC–210, Capitol Visitor Center, Hon. John Ratcliffe (Chairman of the subcommittee) presiding.

Present: Representatives Ratcliffe, Garrett, Fitzpatrick, Donovan, Katko, Langevin, and Jackson Lee.

Mr. RATCLIFFE. The Committee on Homeland Security's Subcommittee on Cybersecurity and Infrastructure Protection will come to order. The subcommittee is meeting today to receive testimony regarding how to maximize the value of cyber threat information sharing. I now recognize myself for an opening statement.

The severity of the threats we face in cyber space can't be overstated. Seemingly, every week there's a new headline about a new breach, a new hack, or a new trove of sensitive information that's been compromised. Or there's a new report highlighting the vulnerabilities of our Government, the private sector, and the American people face from malicious actors.

Those on the operational front of cybersecurity know the threat landscape is evolving at every second. In cyber space, it's nearly impossible to concisely declare who the threat actor is, what they're going to do next, and what the cascading effects may be.

The industry method is to prioritize, assess the risks that networks face and prioritize actions to address those risks, and then keep moving down the list. We in the Government must learn from the private sector, assess risks, prioritize mitigation, and keep moving.

As I've said before, whether we rise up to the challenges in cyber space will play a large part in determining whether America remains the world's superpower.

To effectively address these threats, I couldn't agree more with the consensus opinion that the private sector and the Government need to collaborate. I see a big part of our collective responsibility being to ensure that this collaboration results in not just rhetoric, but in a tangible improvement in our country's cybersecurity posture.

What we're here today to examine is perhaps one of the most readily visible and promising forms of this collaboration: The shar-

ing of cyber threat indicators between the private sector and the Federal Government.

In an ecosystem where there is no silver bullet, it's incumbent upon us to conduct rigorous oversight of our information-sharing programs to help increase the participation in and volume of cyber threat information shared with the private sector.

The private sector is the front line for action in cyber space. In supplying the private sector with an increasing amount of actionable information, we enable our partners to tilt the scales away from our cyber adversaries.

As a committee, we are continually seeking to learn about possible ways that the Department can help to increase the resilience of private-sector networks and fine-tune their own efforts for the response, analysis, and mitigation of cyber threats.

According to DHS, the Automated Indicator Sharing program has shared over 1.3 million unique indicators, more than 264,000 shared in September alone. There are currently 135 non-Federal entities participating in AIS, 22 of which are sector-specific organizations comprised of groups of companies. DHS estimates the actual reach of AIS indicators to be greater than 10,000 organizations.

As encouraging as it is to see these programs take shape and fill the very important role of convening partners and bridging information sharing from the Government to the private sector, we can do better. A recent report from the DHS Office of Inspector General reinforces this notion that there's more work to be done.

Today I look forward to hearing insights and recommendations from our witnesses that we can take back to DHS to continue to strengthen its work sharing cyber threat information. We are tasked with overseeing the crucial DHS programs, knowing that improvements are always possible.

Each of you has a unique perspective that will provide invaluable knowledge that we can build on as DHS continues to refine its programs. We will need creative and possibly significant changes to the way that we do things if we expect to gain ground in this fight.

In a space this transformative and this disruptive, the best option is continued partnership. As disparate as the opinion of the private sector and the Government can be on many issues, when it comes to security, we are all looking for able, willing, and effective partners. The information technology landscape is central to every sector of the economy and every consumer and individual who depend on these systems.

The automation of cyber threat information and the incorporation of Classified and Unclassified information are areas the Government can work on in order to increase the effectiveness of the information being provided to the private sector.

It is for this reason that we have gathered this panel of experts to talk to the efficacy of cyber threat information sharing and improvements that can be made with it. We look forward to hearing from the witnesses, their perspectives and understanding of the current state of cyber threat information sharing, and their vision and their recommendations for a safer future.

Again, thanks to our witnesses for your willingness to share your expertise with us today.

[The statement of Chairman Ratcliffe follows:]

STATEMENT OF CHAIRMAN JOHN RATCLIFFE

NOVEMBER 15, 2017

The severity of the threats we face in cyber space cannot be overstated. Seemingly every week there's a new headline about a new breach, a new hack, or a new trove of sensitive information that's been compromised. Or there's a new report highlighting the vulnerabilities our Government, the private sector, and the American people face from malicious actors.

Those on the operational front of cybersecurity know the threat landscape is evolving at every second. In cyber space it is nearly impossible to concisely declare who the threat actor is, what they are going to do next, and what the cascading effects may be.

The industry method is to prioritize; assess the risks that networks face and prioritize actions to address those risks, and then, keep moving down the list. We in the Government must learn from the private sector, assess risks, prioritize mitigation, and keep moving.

As I've said before—whether we rise up to our challenges in cyber space will play a large part in determining whether America remains the world's superpower.

To effectively address these threats, I couldn't agree more with the consensus opinion that the private sector and Government need to collaborate. I see a big part of our collective responsibility being to ensure that this collaboration results in, not just rhetoric, but, in a tangible improvement to our country's cybersecurity posture.

What we're here today to examine is perhaps one of the most readily visible and promising forms of this collaboration—the sharing of cyber threat indicators between the private sector and Federal Government.

In an ecosystem where there is no silver bullet, it's incumbent upon us to conduct rigorous oversight of our information-sharing programs to help increase the participation in and volume of cyber threat information shared with the private sector.

The private sector is the front line for action in cyber space. In supplying the private sector with an increasing amount of actionable information, we enable our partners to tilt the scales away from our cyber adversaries.

As a committee, we are continually seeking to learn about possible ways that the Department can help to increase the resilience of private-sector networks and fine-tune their own efforts for the response, analysis, and mitigation of cyber threats. According to DHS, the Automated Indicator Sharing program has shared over 1,335,036 unique indicators, 264,234 shared in September alone, and there are currently 135 non-Federal entities participating in AIS, 22 of which are sector-specific organizations comprised of groups of companies. DHS estimates the actual reach of AIS indicators to be greater than 10,000 organizations.

As encouraging as it is to see these programs take shape and fill the very important role of convening partners and bridging information sharing from the Government to the private sector, we can do better. A recent report from the DHS Office of Inspector General reinforces this notion that there is more work to be done.

Today I look forward to hearing insights and recommendations from our witnesses that we can take back to DHS to continue to strengthen its work sharing cyber threat information. We are tasked with overseeing the crucial DHS programs, knowing that improvements are always possible. Each of you has a unique perspective that will provide invaluable knowledge that we can build on as DHS continues to refine its programs. We will need creative and possibly significant changes to the way that we do things if we expect to gain ground in this fight.

In a space this transformative and this disruptive, the best option is continued partnership. As disparate as the opinion of the private sector and the Government can be on many issues, when it comes to security, we are all looking for able, willing, and effective partners. The information technology landscape is central to every sector of the economy and every consumer and individual who depend on these systems.

The automation of cyber threat information and the incorporation of Classified and Unclassified information are areas the Government can work on in order to increase the effectiveness of the information being provided to the private sector. It is for that reason that we have gathered this panel of experts to talk to the efficacy of cyber threat information sharing and improvements that can be made.

We look forward to hearing from the witnesses their perspective and understanding of the current state of cyber threat information sharing and their vision and recommendations for a safer future. Again, thank you to our witnesses for your willingness to share your expertise.

Mr. RATCLIFFE. I now recognize the Ranking Member, my colleague and friend from Rhode Island, Mr. Langevin, for any opening statement that he may have.

Mr. LANGEVIN. Well, thank you, Mr. Chairman.

Good afternoon to our witnesses.

I want to begin by thanking Chairman Ratcliffe for holding today's hearing on cyber threat information sharing and his leadership on this issue more broadly.

Two years ago, Congress passed the Cybersecurity Act of 2015 to remove barriers to fuller and faster cybersecurity threat indicator sharing, both between Government and the private sector and among private entities. This legislation was the result of years of negotiation between experts from industry, academia, private advocates, and security professionals. At the time, there was broad consensus that we were not sharing, analyzing, and integrating data around cyber threats as well as we could be.

To answer this gap in our cybersecurity posture, representatives from both sides of the aisle came together as partners to deliver legislation that removed the legal hurdles that prevented the free flow of threat indicators and to provide liability protections to encourage sharing.

Today those barriers are gone. There are ironclad authorizations for companies to share indicators within industry and back and forth with the Federal Government. There are liability protections to ensure that these actions do not inadvertently put companies at risk. There are even protections on the data themselves to ensure that they are not used for any regulatory action by the Government.

The Cybersecurity Act of 2015 also created a channel for the Government to better disseminate information that would otherwise be Classified. By placing these signals amongst the contributions from all participants, DHS can basically disguise the original sources. During the period of October 2015 to April 2017, the Department shared some 2,290 formerly Classified cyber threat indicators through the Automated Indicator Sharing program, or AIS.

However, despite these advancements, we have a long way to go in operationalizing the law and policy that has been developed. AIS is a good example—is a great example, I should say. Barely more than 100 companies right now have elected to join the program and contribute to the common threat picture, a level of participation that is simply, quite frankly, unacceptable.

Part of this is on the Department, as we have heard numerous times before this committee that the indicators shared by the Government are often late and lack important context. But part of this also falls on industry. After all, with only roughly 100 private-sector participants, it seems many people knocking the data being shared by AIS haven't applied much effort to analyzing the data. 2,290 formerly Classified threat indicators, I believe, certainly count for something.

So that's why I'm grateful to Chairman Ratcliffe and Ranking Member Richmond for continuing to study this issue. We need to know what is and isn't working with the law and with the Department's efforts. We also need to know what activities are being en-

abled that weren't happening before passage of the law and the iron-clad authorizations that I mentioned.

I've said many times that information sharing is not a silver bullet. In fact, there is no such thing in cybersecurity. But I do believe in its promise to help better our cybersecurity posture, and we in Congress owe it to the American people to ensure that we are meeting that potential.

So I will be interested in hearing from the witnesses what we in Congress can do to improve the Department's efforts and to improve uptake among private-sector participants.

Personally, I think that we may need some more assistance from the Department in building a robust ecosystem around the feed rather than just relying on it being out there. I hope the Department looks to the financial sector's expertise, with Soltra Edge for guidance. But I also hope that the private sector, innovative as it is, applies some of the creativity to the data coming out of DHS rather than waiting.

Finally, there are two related issues that I want to mention briefly.

First, I believe that it will be extremely difficult for the Department to make any lasting changes in its policies without permanent political leadership in place. I hope the administration moves swiftly to fill critical vacancies at the National Protection and Programs Directorate. Cybersecurity is a National priority, and the personnel decisions made by the White House need to reflect that.

Second, a brief comment on the new Vulnerabilities Equities Process, or the VEP charter that's released today. Now, I'm grateful that the document continues the presumption of disclosure and ensures a broad array of Government stakeholders, including DHS, have a seat at the table when discussing vulnerabilities.

I'm also pleased by the increased level of transparency indicated by the publication of the charter in Unclassified form and by the annual reports, including to Congress, that it requires.

We owe the selfless Americans who serve their Nation as members of the intelligence community an enormous debt of gratitude, a debt that is far too infrequently acknowledged. As Members of Congress, we also owe them rigorous oversight to ensure that the tools they develop remain secure.

I believe that the VEP is an appropriate process for selecting the very few vulnerabilities where disclosure will be delayed. However, that process falls apart if the exploits cannot be kept in Government hands, and Congress must do more to ensure those safeguards are in place.

So, with that, I'd like to thank the witnesses for being here today. I certainly look forward to discussing ways to improve our collective cybersecurity with all of them.

Before I yield back, Mr. Chairman, I have a letter that I'd like to submit for the record from the Electronic Privacy Information Center on some of these topics as well.

Mr. RATCLIFFE. Without objection, it will be admitted into the record.

[The information follows:]

LETTER SUBMITTED FOR THE RECORD FROM HONORABLE JAMES R. LANGEVIN

NOVEMBER 15, 2017.

The Honorable JOHN RATCLIFFE, Chairman,
The Honorable CEDRIC L. RICHMOND, Ranking Member,
U.S. House Committee on Homeland Security, Subcommittee on Cybersecurity and Infrastructure Protection, H2–176 Ford House Office Building, Washington, DC 20515.

DEAR CHAIRMAN RATCLIFFE AND RANKING MEMBER RICHMOND: We write to you regarding the hearing on "Maximizing the Value of Cyber Threat Information Sharing."[1] EPIC is a public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues.[2] We are particularly interested in the privacy issues raised by the government's cybersecurity policies that implicate the collection and use of personal data.

At the end of 2015, the Cybersecurity Act of 2015 was signed into law.[3] Title of I of that act, known as the Cybersecurity Information Sharing Act of 2015 (CISA), created a mechanism for the Federal Government to disseminate cyber threat information to the private sector and for the private sector to provide cyber threat information to the Federal Government.[4] Much of that information concerns the activities of individual Internet users.

CISA and earlier bills, such as the Cyber Intelligence Sharing and Protection Act (CISPA), were criticized for the potential to compromise American's privacy.[5] With passage of the Cybersecurity Act of 2015, the risk to privacy still remains.[6] The bill relies on a complex procedure to "scrub" identifying information from the computer logs that are turned over by private firms to the Federal Government. This information is explicitly acquired without the privacy safeguards that would otherwise apply under the Federal wiretap.

Effective oversight of the government's collection and use of personal data is particularly important in the realm of cybersecurity where it is easy to obtain vast troves of personal information with little accountability. The history of the U.S. government's surveillance of domestic communications in collaboration with private companies[7] makes it imperative that Congress ensure that CISA safeguards Americans' privacy.

We urge you to ask detailed questions about the dissemination of information from companies to the government, including:

1. What personal information is disseminated to the government in the context of providing cyber threat information?
2. What processes do you use to mitigate the privacy risks before providing cyber threat information to the government?
3. What are the privacy risks with the current mechanism to provide cyber threat information to the government?
4. What more could be done to safeguard the personal data of Americans?

---

[1] *Maximizing the Value of Cyber Threat Information Sharing,* 115th Cong. (2017), H. Comm. on Homeland Security, Subcomm. on Cybersecurity and Infrastructure Protection (Nov. 15, 2017), *https://homeland.house.gov/hearing/maximizing-value-cyber-threat-information-sharing/*.

[2] See *About EPIC,* EPIC.org, *https://epic.org/epic/about.html.*

[3] Consolidated Appropriations Act, 2016, Public Law 114–113, December 18, 2015, 129 Stat 2242, 6 U.S.C. 1501–1510.

[4] Id.

[5] See Jeramie D. Scott, *Cybersecurity: the view from Washington,* Daily Journal (Jan. 28, 2015), available at *https://epic.org/epic/jeramie-scott-cybersecurity-oped.pdf;* Wired staff, *CISA Security Bill Passes Senate With Privacy Flaws Unfixed,* Wired (Oct. 27, 2015), *https://www.wired.com/2015/10/cisa-cybersecurity-information-sharing-act-passes-senate-vote-with-privacy-flaws/;* Danny Weitzner, *The New US Cybersecurity Bill Will Invade Your Privacy, But It Won't Keep You Safe,* Quartz (Nov. 8, 2015), *https://qz.com/543692/americans-should-probably be-more-freaked-out-about-that-new-cybersecurity-bill/*.

[6] See Taylor Armerding, *Information Sharing Bill Passes, But Privacy Debate Goes On,* CSO (Jan. 14, 2016), *https://www.csoonline.com/article/3021907/security/information-sharing-bill-passes-but-privacy-debate-goes-on.html.*

[7] EPIC, *EPIC v. Hemisphere, https://epic.org/foia/dea/hemisphere/*.

We ask that this letter be entered in the hearing record. EPIC looks forward to working with the Subcommittee on these issues of vital importance to the American public.

Sincerely,

MARC ROTENBERG,
EPIC President.
CAITRIONA FITZGERALD,
EPIC Policy Director.
JERAMIE SCOTT,
EPIC National Security Counsel.

Mr. LANGEVIN. Thank you, Mr. Chairman. I yield back.
[The statement of Hon. Langevin follows:]

STATEMENT OF HONORABLE JAMES R. LANGEVIN

NOVEMBER 15, 2017

Two years ago, Congress passed the Cybersecurity Act of 2015 to remove barriers to fuller and faster cybersecurity threat indicator sharing both between Government and the private sector and among private entities.

This legislation was the result of years of negotiation between experts from industry, academia, privacy advocates, and security professionals. At the time, there was broad consensus that we were not sharing, analyzing, and integrating data around cyber threats as well as we could be.

To answer this gap in our cybersecurity posture, Representatives from both sides of the aisle came together as partners to deliver legislation that removed the legal hurdles that prevented the free flow of threat indicators and to provide liability protections to encourage sharing.

Today, those barriers are gone. There are iron-clad authorizations for companies to share indicators within industry and back and forth with the Federal Government. There are liability protections to ensure that these actions do not inadvertently put companies at risk. There are even protections on the data themselves to ensure that they are not used for any regulatory action by the Government.

The Cybersecurity Act of 2015 also created a channel for the Government to better disseminate information that would otherwise be Classified. By placing these signals amongst the contributions from all participants, DHS can disguise the original sources. During the period of October 2015 to April 2017, the Department has shared 2,290 formerly Classified cyber threat indicators through the Automated Indicator Sharing program, or AIS.

However, despite these advancements, we have a long way to go in operationalizing the law and policy that has been developed.

Barely more than 100 companies have elected to join the program and contribute to the common threat picture, a level of participation that is simply unacceptable.

Part of this is on the Department, as we have heard numerous times before this committee that the indicators shared by the Government are often late and lack important context.

But part of this also falls to industry—after all, with only roughly 100 private-sector participants, it seems many people knocking the data being shared by AIS haven't applied much effort to analyzing the data. Two-thousand two hundred formerly Classified threat indicators certainly count for something.

That is why I am grateful to Chairman Ratcliffe and Ranking Member Richmond for continuing to study this issue. We need to know what is and isn't working with the law and with the Department's efforts. We also need to know what activities are being enabled that weren't happening before passage of the law and the iron-clad authorizations I mentioned.

I have said many times that information sharing is not a silver bullet—in fact, there is no such thing in cybersecurity. But I do believe in its promise to help better our cybersecurity posture, and we in Congress owe it to the American people to ensure we are meeting that potential.

So I will be interested in hearing from the witnesses what we in Congress can do to improve the Department's efforts and to improve uptake among private-sector participants.

Personally, I think that we may need some more assistance from the Department in building a robust ecosystem around the feed—rather than just relying on it being out there—and I hope the Department looks to the Financial Sector's experience with Soltra Edge for guidance.

But I also hope that the private sector, innovative as it is, applies some of the creativity to the data coming out of DHS rather than waiting.

Finally, there are two related issues that I want to mention briefly.

First, I believe it will be extremely difficult for the Department to make any lasting changes in its policies without permanent political leadership in place, and I hope the administration moves swiftly to fill critical vacancies at the National Protection and Programs Directorate. Cybersecurity is a National priority, and the personnel decisions made by the White House need to reflect that.

Second, a brief comment on the new Vulnerabilities Equities Process (VEP) Charter released today. I am grateful that the document continues the presumption of disclosure and ensures a broad array of Government stakeholders, including DHS, have a seat at the table when discussing vulnerabilities. I am also pleased by the increased level of transparency indicated by the publication of the Charter in Unclassified form and by the annual reports, including to Congress, it requires.

We owe the selfless Americans who serve their Nation as members of the intelligence community an enormous debt of gratitude, a debt that is far too infrequently acknowledged. As Members of Congress, we also owe them rigorous oversight to ensure the tools they develop remain secure. I believe that the VEP is an appropriate process for selecting the very few vulnerabilities where disclosure will be delayed. However, that process falls apart if the exploits cannot be kept in Government hands, and Congress must do more to ensure those safeguards are in place.

With that, I would like to thank the witnesses for being here today, and I look forward to discussing way to improve our collective cybersecurity with them.

Mr. RATCLIFFE. I thank the gentleman.

Other Members of the committee are reminded that opening statements may be submitted for the record.

[The statements of Ranking Member Thompson and Honorable Jackson Lee follow:]

STATEMENT OF RANKING MEMBER BENNIE G. THOMPSON

NOVEMBER 15, 2017

When this committee was formed, the Nation was still reeling from the September 11, 2001, attacks, and the difficult reality that there were significant information-sharing gaps between our intelligence services and law enforcement.

In the months the followed 9/11, the Bush White House warned of "invisible enemies that can strike with a wide variety of weapons" and urged the Congress to stand up a consolidated Department of Homeland Security to protect against the known threats of the day and the unknown threats of the future.

Fifteen years later, the threat landscape has changed dramatically. The "invisible enemies" we face are hackers hiding in plain sight, casing our networks to figure out how to penetrate deeper, steal data, and manipulate networked systems. Fortunately, we do not need to relearn the lessons that 9/11 taught us.

We know that information sharing—in this case, among the public and private sector—can help mitigate or even prevent cyber intrusions. And the Cybersecurity Act of 2015 put in place the mechanisms necessary to facilitate and incentivize robust information sharing. That said, the more things change, the more they stay the same.

After 9/11, we had to overcome an initial reluctance among the intelligence community and law enforcement to liberally share threat information with other agencies that needed to know.

Among other things, information sharing struggled to overcome challenges related to turf wars, fear of reputational damage, and balancing the need to protect information and the need to share it so law enforcement would be able to act.

Similarly, today DHS is struggling to incentivize private-sector participation in its cyber threat information-sharing platforms, despite Congress acquiescing to demands for strong liability protections.

We hear from stakeholders that the information shared is not actionable, that too much of the information necessary to make indicators actionable is Classified, and that there is a lack of confidence in the validity of some indicators because of a lack of adequate vetting.

These are all issues that Federal, State, and local law enforcement had to overcome in the years following 9/11, and, with the help of Congress and DHS, they have made tremendous progress.

I have every confidence that the same will be true for cyber threat information sharing.

That said, I am concerned that we continue to hear the same pattern of criticisms over DHS cyber threat information products, and I will be interested to know how DHS solicits and incorporates feedback into its programs, from Automated Indicator Sharing (AIS) to the Cyber Information Sharing and Collaboration Program.

I also look forward to hearing from witnesses how DHS can attract better participation non-Federal network owners and operators, who control 80 percent of our Nation's networks.

I have heard some concerns that potential participants are holding out until DHS's programs prove greater value, but I would caution that DHS's voluntary programs are only as good as the participants make them. If the private sector refuses to participate in two-way information sharing, DHS's are doomed to fail.

STATEMENT OF HONORABLE SHEILA JACKSON LEE

NOVEMBER 15, 2017

Chairman Ratcliffe and Ranking Member Richmond, thank you for convening today's hearing of the Homeland Security Committee Subcommittee on Cybersecurity & Infrastructure Protection on the topic of "Maximizing the Value of Cyber Threat Information Sharing."

Today's hearing will give Members an opportunity to hear from stakeholders to learn their perspectives on the Department of Homeland Security's (DHS) execution of its cyber threat information-sharing responsibilities as established by the Cybersecurity Act of 2015.

I look forward to hearing from today's witnesses:

- Anne Barron-DiCamillo, vice president, cyber threat intelligence and incident response, American Express;
- Trish Cagliostro, Federal solutions architect manager, Anomali;
- Robert Knake, senior research scientist, Northeastern University Global Resilience Institute; and
- Robert Mayer, senior vice president, cybersecurity, US Telecom Association (Democratic witness).

Today presents an important opportunity to engage stakeholders on private-sector reluctance to participate in DHS's Automated Indicator Sharing (AIS), and how DHS can improve confidence in its cyber threat information work that is being shared with private industry.

The information shared is only as good as the level of trust that is put on it by the intended audience.

We need to understand how the cybersecurity work of DHS is perceived.

Over the past year, Russian actors targeted U.S. election infrastructure, hackers escalated efforts to breach the domestic energy sector, and WannaCry and NotPetya ransomware wreaked havoc on public and private infrastructure around the world.

According to Symantec, "The world of cyber espionage experienced a notable shift toward more overt activity, designed to destabilize and disrupt targeted organizations and countries."

Protecting against these growing cyber threats will require public and private-sector entities to share cyber threat and incident information that is timely and actionable.

DHS CYBER ASSETS

The NPPD Office of Cybersecurity & Communications (CS&C), specifically the National Cybersecurity and Communications Integration Center (NCCIC), carries out the bulk of the DHS responsibility of facilitating the sharing of cyber threat information.

Although DHS is authorized to deploy a range of tools, resources, and programs to carry out its cyber mission, it has limited authority to regulate privately-owned networks and cannot require private entities to adopt specific security measures, grant access to their systems, or share information.

Instead, the success of DHS efforts relies on voluntary participation from the private sector.

DHS voluntary cyber threat information-sharing programs include:

- Cyber Information Sharing and Collaboration Program (CISCP);
- Enhanced Cybersecurity Services (ECS); and
- Automated Indicator Sharing (AIS).

DHS must be prepared to collect analysis and deliver actionable information that is relevant to the industry or entity who is the intended audience.

The bulk of our Nation's critical infrastructure is owned and controlled by the private sector.

The partnership to protect the electric grid, water systems, mass transit systems, and the telecommunication networks must be a partnership that works well for the private and public sector.

Earlier this year, the full Homeland Security Committee marked up H.R. 3202, the Cyber Vulnerability Disclosure Reporting Act.

This bill seeks a report on the Department of Homeland Security's policies and procedures for coordinating cyber vulnerability disclosures such as Zero Day Events with private-sector partners.

The Jackson Lee cybersecurity information-sharing bill requires the Secretary of Homeland Security to submit a report on the policies and procedures developed for coordinating cyber vulnerability disclosures.

The report will include an annex with information on instances in which cybersecurity vulnerability disclosure policies and procedures were used to disclose details on identified weaknesses in computing systems or digital devices at risk.

The report also provides information on the degree to which the information provided by DHS was used by industry and other stakeholders.

The report may also contain a description of how the Secretary of Homeland Security is working with other Federal entities and critical infrastructure owners and operators to prevent, detect, and mitigate cyber vulnerabilities.

The reason that I worked to bring this bill before the committee is the problem often referred to as a "Zero Day Event," that describes the situation that network security professionals may find themselves when a previously-unknown error in computing code is exploited by a cyber criminal or terrorist.

The term "Zero Day Event" simply means that there is zero time to prepare a defense against a cyber attack.

Cyber attacks that target computer networks or computing devices primarily focus upon exploiting errors in computing code.

If the defect in software is discovered by network engineers and software development companies can work to develop a "patch" to fix the problem before it can be exploited by those who may seek to do harm.

Because vulnerabilities can be used by adversaries it is important that this sensitive information be managed securely so details are not routinely made available neither to the public nor to Congress.

This bill will provide the committee with the opportunity to understand the process and procedures used by the Department of Homeland Security and the benefit these disclosures may have for private-sector entities participating in programs in support of cybersecurity.

I look forward to hearing from today's witnesses.

Thank you.

Mr. RATCLIFFE. We are very pleased to have a very distinguished panel of witnesses before us today on this important topic.

Mr. Robert Knake is the Whitney Shepardson senior fellow at the Council on Foreign Relations and is testifying today on behalf of the Global Resilience Institute.

Welcome to the committee, Mr. Knake.

Ms. Ann Barron-Dicamillo is the vice president of cyber intel & incident response at American Express.

We're glad to have you with us today as well.

Ms. Patricia Cagliostro is the Federal solutions architect manager at Anomali.

Thanks for agreeing to testify today.

Finally, Mr. Robert Mayer is the senior vice president for cybersecurity at the USTelecom Association.

Mr. Mayer, welcome to you as well.

I'd now ask the witnesses to stand and raise your right hand so I can swear you in to testify.

[Witnesses sworn.]

Mr. RATCLIFFE. The witnesses' full written statements will appear in the record.

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

STATEMENT OF ROBERT K. KNAKE, WHITNEY SHEPARDSON SENIOR FELLOW, COUNCIL ON FOREIGN RELATIONS, ON BEHALF OF THE GLOBAL RESILIENCE INSTITUTE

Mr. KNAKE. Thank you, Chairman Ratcliffe. Thank you, Ranking Member Langevin, and distinguished Members of the committee.

I want to start out by saying that I think we've made tremendous progress on this issue over the last 5 years in particular. I would recognize the Cyber Information Sharing Act of 2015 as really having cleared the underbrush on cybersecurity information sharing. There really should no longer be any reason why a company says they cannot legally share information.

So I think we've done that. I'm proud to have supported that work when I was working in the Obama administration, and had always a very good relationship with your committee and your staff members.

Now I think the question is not how do we get rid of disincentives, but how do we incentivize sharing and how do we put in place the mechanisms we need to make information sharing possible?

I'd focus on two areas. The first is I think that we've already done almost everything we can to declassify information for information sharing. I think Classified information exists for a reason. It needs to be protected. Yet at the same time, many private-sector companies that operate critical infrastructure need that information.

So the only way that we can solve that problem is if we extend Classified connectivity for information sharing to critical infrastructure companies. That would, I think, be a very significant move that also has strong precedent. The Department of Defense has operated something called the Defense Industrial Base Network now since 2008. They've shown that it is possible to share Classified information with private companies for their own defense.

I think what we need to do on this topic is to create something that I'll call CInet, or Critical Information Network, with a Classified component and share that with, I would say, the section 9 companies under Executive Order 13636 to start. Those companies, I think, have been recognized as facing a severe threat from our Nation's adversaries and they need to be brought into that Classified network.

So I think we could do that under existing authorities that Congress has granted to the Secretary of Homeland Security and that the President has already extended to the Secretary. I think that is entirely possible and achievable. I'd recommend that we proceed with a pilot effort in that regard. I think it could be done for a limited amount of money and under existing authorities.

The second topic that I'll touch on just briefly is the need for what people call a NTSB for cybersecurity, a National Transportation Safety Board for cybersecurity. This is the idea that when

a plane crashes, investigators show up and they immediately try and find, why did a plane go down, why did a train derail?

In cybersecurity, we need that. When an incident happens, what everybody wants to know is why did it happen and what can they do to protect themselves, were they affected by the same incident, were they targeted by the same adversaries? We have no mechanism to do that now other than leaks and media reports and rumor, innuendo, and surmise.

From my perspective, the appropriate way to do this is not to take this NTSB analogy too far. That's a Government mandate. That's a regulated program. Rather, what I'd like to see is a voluntary effort that is possibly advocated for or created by DHS, but led with the private sector, that I think is backed by insurance, where you would get the equivalent of an insurance discount if you agree to have investigators come in, figure out what went wrong, and share that information, possibly anonymously, with the rest of the sector.

I think if we had that kind of setup and that pre-commitment to engaging in this way, we'd be able to get the most valuable information out of a company that's been targeted by these adversaries. If you were able to do that, I think you would address one of the hardest problems in information sharing, which is the fact that if you have been targeted, sharing information about that doesn't help you, it helps everybody else. It's a tragedy of the commons. I think a program like that would overcome those hurdles.

So I'll stop there. Thank you for the invitation today.

[The prepared statement of Mr. Knake follows:]

PREPARED STATEMENT OF ROBERT K. KNAKE

NOVEMBER 15, 2017

INTRODUCTION

Thank you Chairman Ratcliffe, Ranking Member Richmond, and Members of the committee for the opportunity to testify on this important matter. While much work remains to be done, I believe it is important to start by noting that much has been accomplished. Information sharing has been the focus of the cybersecurity community for the better part of a decade and has enjoyed bipartisan support.

When I was director for cybersecurity policy at the National Security Council from 2011 to 2015, I had a productive bipartisan working relationship with Congress that resulted in several successful pieces of legislation. Important with respect to the topic of today's hearing, was the passage of the Cybersecurity Information Sharing Act of 2015 that succeeded in resolving many of the reasons private companies believed they were unable to participate in cybersecurity information sharing. By explicitly offering liability protections and other safeguards, CISA has removed major barriers to information sharing.

The primary challenges that remains are creating meaningful incentives whereby the sharing of cyber threat information has real value for network defenders and providing a secure operational environment for allowing the most sensitive information to be shared. In my testimony today, I will focus on two areas that I believe deserve the committee's attention: (1) The need for a secure network for Classified information sharing, collaboration, and operations for use by critical infrastructure; and 2) the need for a mechanism to quickly investigate and share information on the causes of cyber incidents.

DEVELOPING A SECURE NETWORK FOR CLASSIFIED INFORMATION SHARING, COLLABORATION, AND OPERATIONS

Through programs like Automated Indicator Sharing (AIS) and the Cyber Information Sharing and Collaboration Program (CISCP), the Department of Homeland Security is fulfilling its mandate to broadly share information the Government has

with private companies and State, local, territorial, and Tribal governments that need it to protect themselves. When combined with vendor products and private-sector collaboration through Information Sharing and Analysis Centers, Information Sharing and Analysis Organizations, and efforts such as the Cyber Threat Alliance, these programs meet the needs of most companies.

Yet, Government policy recognizes that a small set of private companies that operate the Nation's critical infrastructure are under near-constant threat from sophisticated actors. These "Section 9 list" companies (those identified pursuant to Section 9 of Executive Order 13636), require the ability to communicate with the Government over Classified channels in order to protect the Nation's critical infrastructure from our adversaries.

Solutions to the problem of Classified information sharing to date have been partial at best. Federal agencies continue to try and declassify or "tearline" more cyber threat information, separating out actionable threat information from intelligence. Federal agencies are also routinely providing Classified in-person briefings to cleared individuals in the private sector.

These measures can never fully address the challenge of providing detailed and timely information to key infrastructure owners and operators. Given the clear and present on-going threat of cyber attacks, Section 9 companies must be able to receive Classified threat information in real time and to be able to coordinate securely with Government and other private companies on network defense. What they need is a Classified network for sharing critical infrastructure information. In addition to information sharing on cyber threats, I believe that such a network could address two other challenges.

President Eisenhower famously said, "If a problem cannot be solved, enlarge it." There is a tendency to view the idea of a Classified network for critical infrastructure as too costly and difficult to manage for the value it would provide. As one Government leader who considered the topic asked, "is the juice worth the squeeze?" My answer to that is an emphatic yes. The Government owes it to its partners in the private sector to provide them the detailed and timely intelligence that they need to protect themselves and this cannot be done in Unclassified form; Providing a Classified network for Section 9 companies would help to ensure a higher degree of assurance for critical infrastructure operations and provide a necessary fall-back communications system in the event that the public internet is disrupted. Given the on-going threat and the significant economic and security consequences associated with disrupting the Nation's critical infrastructure, there is ample justification to develop a new network.

Sharing Classified Information and Threat Collaboration

When the Government has information that private companies need to protect themselves, it has an obligation to provide that information. A duty to warn exists as one of the rationales for the collection of intelligence and is embedded in the authorities granted to the Department of Homeland Security at its creation. To this end, the intelligence community, the FBI, and DHS deserve credit for initiating a program in 2013 to provide notification to private companies if they were the victim or target of malicious cyber activities. Government notification is now one of the leading ways that companies discover cyber incidents.

Through this program and related efforts, the Government has wrestled with the challenge of sharing Classified information with private companies. De-classification remains a slow and cumbersome process in large part because there is, in most cases, a good reason that Classified information should not be put into the public realm.

When information cannot be declassified, Government agencies have attempted to address the challenge in two ways. Through in-person briefings, they convey information to cleared personnel at relevant companies. These briefings are valuable for raising awareness but are not useful for operational purposes. The Enhanced Cybersecurity Services (ECS) program attempted to address the operational challenges associated with Classified information by deploying Classified signatures to managed security service providers that could be used to block attacks. ECS, based on a successful pilot effort within the Defense Industrial Base (DIB), is certainly part of an overall solution.

What ECS does not provide is context and multi-party communication. A signature alone is not sufficient to protect companies. Organizations under threat from the Nation's adversaries need to understand who is targeting them, why they are being targeted, how to protect themselves against the threat, and what threat actors may do next.

The Department of Defense has largely solved this problem for DIB companies. DoD successfully piloted and moved into production the Defense Industrial Base

Network (DIBnet), a Classified network for communicating with DIB companies. The network is used both to share Classified information on threats and to securely convene to coordinate incident response. For DIB companies, DoD has shown the importance of being able to deploy both Classified indicators and to communicate the context around threats. The DIBnet concept should be extended by the Department of Homeland Security to other critical infrastructure sectors.

Several colleagues of mine and I worked with the Intelligence and National Security Alliance (INSA) to develop a proposal for creating a Classified network for sharing Classified information and threat collaboration for the financial services industry based on DIBnet. I have included the paper, "FINnet: A Proposal to Enhance the Financial Sector's Participation in Classified Cyber Threat Information Sharing" for the record.

In the paper, we argue that the authority to establish a Classified network for critical infrastructure is already vested in the President and the Secretary of Homeland Security. Executive Order 13691 of February 13, 2015 "Promoting Private Sector Cybersecurity Information Sharing" gave the Secretary of Homeland Security the necessary authority to establish a Classified network for critical infrastructure companies. That order also directed the updating of the National Industrial Security Program Operating Manual (known as "the NISPOM") to better accommodate the needs of private companies that are not part of the Defense Industrial Base. Congress followed this action by charging the Federal Government with developing mechanisms to allow for "the timely sharing of Classified cyber threat indicators and defensive measures in the possession of the Federal Government with representatives of relevant Federal entities and non-Federal entities that have appropriate security clearances . . . " as part of CISA.[1]

We believe that DHS, Treasury, FBI, and Secret Service should work together to pilot the FINnet concept with a small number of financial services firms that have mature security organizations and are willing participants. Companies from other sectors could also be brought into the pilot. This pilot should be launched right away and initially operate at the Secret level, using secure phones, laptops, and encryption cards to communicate securely over the public network infrastructure. If the pilot is successful, it could be migrated to dedicated network infrastructure that would provide higher degrees of assurance.

Crucial to the success of the DIBnet is that it is backed by the Defense Cyber Crime Center (DC3). DC3 provides companies connected through the DIBnet with "analytic support, incident response, mitigation and remediation strategies, malware analysis, and other cybersecurity best practices to participating companies."[2] In short, DC3 takes a customer service approach to the DIB. It fosters information sharing among participating companies by providing valuable services when companies share information with it. Such an approach is critical to replicating the success of the DIBNet for other sectors. Each sector needs a Government partner with a deep understanding of its sector, strong relationships with members of the sector, and the ability to provide value back to participating companies when they share information.

Protecting Critical Infrastructure Operations

The second challenge that such a network should address is the protection of critical infrastructure operations. As critical infrastructure grows more dependent on information technology, particularly given the growth of the so-called "Internet of Things", companies are connecting their operational technology to the public internet. While it is economical to use the public internet for this purpose, the risk that critical infrastructure could be disrupted through a cyber attack highlights the need for higher levels of assurance provided by a separate network. As the National Infrastructure Advisory Council (NIAC) concluded in its latest report, "Industrial control systems connected to business IT systems and the Internet constitute a systemic cyber risk among critical infrastructure."[3]

The NIAC report recommends the establishment of "separate, secure communications networks specifically designated for the most critical cyber networks, including 'dark fiber' networks for critical control system . . . ". The NIAC called for a pilot project to identify dark fiber that could be used for the network and test whether critical infrastructure could be operated if separated from the public network. Some

---

[1] 6 USC 1502.

[2] Office of the Director of National Intelligence, Department of Homeland Security, Department of Defense, and Department of Justice, "Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government Under the Cybersecurity Information Sharing Act of 2015," February 16, 2016, page 8.

[3] *https://www.dhs.gov/sites/default/files/publications/niac-securing-cyber-assets-final-report–508.pdf*.

utilities have already begun to migrate their operations to dedicated networks that they own instead of continuing to use the public internet. Piloting this concept is well warranted given the threats our connected infrastructure faces.

Coordinating Network Restoration

The third problem that such a network could address would be coordinating network restoration in the event of an attack that destabilizes the public internet. While the internet has grown increasingly robust, it is not immune from disruptive cyber attacks. Some botnets have grown so large that a distributed denial-of-service attack could take down portions of the network. They have become so sophisticated that it can be difficult for network operators to separate the signal from the noise and filter out the attacks.

In the period after 9/11, the Bush administration recognized the need to have a backup, redundant communications system to coordinate network restoration in the event of an internet outage. The Critical Infrastructure Warning Information Network (CIWIN) was created with two purposes: It would serve on a daily basis to provide information on threats to critical infrastructure and provide a back-up communications capability in the event of an internet outage.

CIWIN ran over the internet's physical infrastructure but on dedicated circuits that would allow users to continue to communicate as long as the core routing infrastructure was still operational. In the face of budget cuts, the Department of Homeland Security canceled the program in 2013. The system had not been routinely exercised and no information was flowing over it.

The need for such a system remains. The problem with CIWIN was that the information that was shared over it was Unclassified and could also be shared over the public internet so it was essentially a redundant network that would only be used if the public internet was compromised. However, the need to routinely share Classified information would mean the network would be used on a daily basis as part of operations. Business needs will dictate use of the most expedient medium for sharing information. Absent the presence of Classified information that cannot legally be shared on enterprise networks, operators will routinely fall back to sharing over Unclassified email, phone, and other systems.

Taken together, I believe that the need to share Classified threat information, the need to provide higher levels of assurance for critical infrastructure operations, and the need for a redundant communications system in the event of an internet outage amply justifies the development of a dedicated secure network.

CREATING A "NATIONAL TRANSPORTATION SAFETY BOARD" FOR CYBER INCIDENTS

Over the last decade, cybersecurity professionals have recognized that, try as they might, incidents will still occur. The concept of "cyber resilience" is emerging to capture the idea that, while we may not be able to stop all harms from occurring in cyber space, we can rapidly respond, recover, and adapt, becoming stronger than we were before. Achieving resilience, however, is not something any individual organization can do alone. Instead, it requires a collective effort so that the lessons learned from an individual incident at a company are widely disseminated and countermeasures implemented.

While a small number of defense contractors and financial services firms have recognized that sharing this kind of information is vital and, if done in the proper context, does not introduce risk to the firm, most companies fear the downside of sharing and see no potential upside. Companies fear that sharing information about a breach, even if it did not result in the loss of any data, will cause a public relations nightmare and result in a loss of stock value. It could lead to the firing of the CISO and even CEO. Even if these concerns were addressed, that would simply mean that there is limited downside. It would not mean that there is an upside or any kind of positive incentive to share this information. After all, sharing this kind of information does not directly help the company that has been breached; it only helps other companies detect or prevent a breach. Simply put, the challenge for information sharing is that the last thing a company that has experienced a breach wants to do is tell anybody else that it happened, let alone how it happened. Yet, it is in the National security interest that they do so as soon as possible.

To address this problem, many in the security community have long advocated for the equivalent of the National Transportation Safety Board (NTSB). When a plane crashes or a train derails, NTSB shows up on the scene to investigate. The goal of NTSB is not to assign blame but to figure out what went wrong and to rapidly develop recommendations to prevent an incident like that from ever happening again. This information and those recommendations are rapidly shared with other airlines who quickly work to implement them. Such a virtuous cycle is what we need in cyber.

The challenge is that a plane crash is a public event and a cyber incident is usually, at least initially, a private one. An NTSB for cyber incidents requires a new system of notification and disclosure. It also requires developing a rubric under which companies that are busy trying to contain an incident are also willing to cooperate with an investigation that is not about helping them but about helping everyone else learn from their mistakes. Constructing such a system is no simple task.

A straightforward approach, which I do not recommend, would require disclosure of breaches to the Federal Government and would give a Government agency the authority to investigate and disseminate lessons learned. I do not believe such an approach I do not believe would be in the spirit of the public-private partnership we have worked to construct over the last two decades. It would create an adversarial relationship to the detriment of the cooperative environment we need to foster.

Instead, I believe what is necessary is a voluntary program under which companies are incentivized to agree that in the event of incident they will disclose it and cooperate with investigators that have a mission to surface and share the causes of the incident with the rest of the community.

One option that has worked well in a few incidents is to have US–CERT accompany the FBI on the bureau's investigation to advise the firm on "asset response" with a secondary purpose of collecting and sharing information for dissemination. The challenge with this approach is that companies may not cooperate with law enforcement investigations and often have little interest in receiving assistance from the Government.

In my view, a better approach is to use cyber insurance to establish an obligation to disclose and to allow an independent investigation into the causes of the incident to take place for the purpose of disseminating that information to other companies. Such a system need not require public disclosure of either the fact of the breach or the findings. A Council on Foreign Relations paper that I authored on, "Creating a Federally-Sponsored Cyber Insurance Program,"[4] called for an NTSB-like program be established as a requirement for participation in any Federally back-stopped cyber insurance program.

While I support this recommendation, I do not believe that a Government-backstopped program must be a prerequisite for advancing this kind of information sharing. Insurance companies, if they banded together, could set participation in this kind of disclosure and investigation program as a requirement for their underwriting commercially available insurance or in order to receive a discount on policies. Doing so would be in the interest of insurance companies, as it would help to reduce their aggregate risk by speeding the containment of related breaches that may yet to be discovered.

Congress should work with the insurance industry to identify whether there are any legal impediments to establishing this sort of program.

WHAT WE ARE DOING AT NORTHEASTERN UNIVERSITY

I recently joined the Global Resilience Institute (GRI) at Northeastern University. GRI's mission is to is to lead a university-wide interdisciplinary effort to advance resilience-related initiatives that contribute to the security, sustainability, health, and well-being of societies. As with all efforts to create and sustain global change, they must start locally. Thus, we are working within the metro-Boston area to bring together the stakeholders who are willing to develop, test, and pilot the concept of a secure, redundant communications system that could be used for information sharing, collaborating on incident response, and restoring public networks should they become inoperable or compromised.

Mapping Critical Infrastructure and Dark Fiber in the Boston Area

We are beginning this effort by developing a map of critical infrastructure in the metro-Boston area. Initially, because of the challenges associated with getting detailed infrastructure information, this will not be a comprehensive model, but it will provide a foundation for identifying critical assets that can potentially be connecting to the available dark fiber in the Boston area. This will allow us to identify the practical barriers for making these connection, focusing in particular on the "last mile" challenge—how much additional fiber would need to be strung to connect control systems to the network. Our initial assessment suggests that the costs are likely to be significantly lower than many expect.

---

[4] *https://www.cfr.org/report/creating-federally-sponsored-cyber-insurance-program.*

Technical Design of a Secure Network

We have also begun work to design the architecture for this network. As indicated elsewhere, a dark fiber network is the preferred option at this stage; however, we are investigating other transmission mediums for where fiber is either not practical or desirable. For instance, long-distance transmissions in rural areas might suggest microwave or other "over the air" technologies; likewise, in a coastal area like Boston, an over-the-air system might prove more resilient than fiber running underground or strung on telephone poles.

While it is tempting to think of a secure network as a closed loop, such a network would have limited use. Data will need to be securely moved on and off the network. For cybersecurity operations, incident data will need to be pulled up from the public internet or enterprise business networks to be analyzed. Indicators of compromise extracted through analysis will need to be pushed down to be of use to network defenders. For industrial control systems, while communications with operations centers could take place on the closed network, signals from devices (at homes for instance) will need to be pulled up. Thus, it will be essential that the network allows, but strictly limit and monitor, communications to and from untrusted sources on the internet.

The secure movement of data on and off the network can be accomplished with a series of "guards" or "cross domain solutions" that are used in Government systems to move data from Unclassified domains to Classified domains. We are exploring the commercial application of these technologies and believe a viable system can be developed.

Admittedly, a perimeter approach such as we are advocating here is not a silver bullet. In fact, it has become popular in the cybersecurity community to declare that "the perimeter is dead". We think that such a notion is more marketing hype than reality for most companies. In the critical infrastructure space, it would not be responsible risk management to give up on limiting access to connected devices. Yet, we recognize that a "hard exterior" and "soft middle" is not the right solution. Even a separate network with the most advanced cross-domain solutions and best inspection technologies can be breached. We are also painfully aware of the risk of insider threats, particularly when dealing with industry. Thus, the design of the network needs to account for both the threat from external actors as well as malicious insiders.

To address insider threats or to detect external threats that have compromised the security of the network, we believe that it is possible to develop a viable approach that will take advantage of new technologies that have been difficult or costly to implement in legacy networks. On a basic level, advances in software-defined networking and related technologies can allow the segmentation of traffic at multiple classifications. The network could easily accommodate Sensitive But Unclassified operational communications for critical infrastructure as well as Classified communications on cyber threats for network defenders. Traffic moving across the network can be inspected, not just on exit and entry, and data accessed by users tracked to monitor for potential malicious conduct. In short, advances in technology together with the proper governance structure can limit access to data to those who need to know. Objections to extending this connectivity to the private sector based on concerns over security can be effectively addressed.

Business Model

As we have begun to develop this concept, a persistent question has been raised that should be familiar to all Members of the committee: Who will pay for it? I generally tend to favor the view that the necessary investment for cybersecurity is best treated as the cost of doing business for modern enterprises; however, I believe it is unlikely that the private sector will fund the development of a secure network on its own. A model in which the Government selects an independent network operator and pays the initial cost of a pilot project that guides the development of the network is likely the most viable path. After it is established, use of it by critical infrastructure companies could incur a fee to cover its costs. The process for selecting the Electric Reliability Organization established by the Energy Policy Act of 2005 may be a model worth investigating.

Next Steps

As we continue to develop the concept of a Classified network for critical infrastructure, we will look for opportunities to collaborate with critical infrastructure companies in the metro-Boston area and beyond. Our plan is to be able to present a feasibility study on this topic within the next 6 months and to engage in a regional pilot within a year.

CONCLUSION

Thank you for the opportunity to testify on these important issues. As I hope my testimony conveyed, I believe that the remaining challenges in information sharing require identifying discrete problems and working to collaboratively develop specific solutions. As we pursue the development of these solutions and identify roadblocks, I look forward to continuing to engage with you, your staff members, and with my colleagues in the Executive branch to further develop these important concepts.

I would be happy to answer any questions at this time.

Mr. RATCLIFFE. Thank you, Mr. Knake.

The Chair now recognizes Ms. Barron-Dicamillo—did I say that right?

Ms. BARRON-DICAMILLO. Yes, you did, sir.

Mr. RATCLIFFE. For her opening statement.

STATEMENT OF ANN BARRON-DICAMILLO, VICE PRESIDENT, CYBER INTEL & INCIDENT RESPONSE, AMERICAN EXPRESS

Ms. BARRON-DICAMILLO. Thank you, Chairman Ratcliffe, Ranking Member Langevin, and Members of the subcommittee. My name is Ann Barron-Dicamillo, and I am vice president of cyber intelligence and incident response at American Express. Thank you for this opportunity to be here today. I really look forward to the discussion.

In my role at American Express, I'm responsible for managing cybersecurity operations and directing cyber threat intelligence globally for the company. Prior to my role at American Express, I was director of US–CERT at Homeland Security. My responsibilities there included leading cybersecurity incident response activities, as well as sharing relevant data from those events with both public and private-sector companies on cyber threat information-sharing initiatives.

While at DHS, I engaged in efforts to mature public-private cyber threat intelligence information-sharing programs like those encouraged by CISA. This legislation really helped address many of the concerns that I experienced while I was there around critical infrastructure sector partners, including American Express, engaging in cyber threat information sharing with the Government. It created the ability for DHS to establish machine-speed sharing, while protecting enterprises from associated liability concerns.

One program worth discussing today, which was already mentioned by the Chairman, is AIS. AIS has had limited adoption to date and early challenges in demonstrating its full potential, as was mentioned by the Ranking Member.

While AIS may be a good program for new entrants into the cyber information-sharing community, it would be more effective for more mature organizations in the broader critical infrastructure community if it offered three key things, and two of them were also mentioned by the Ranking Member: Timelier indicator sharing, richer context around indicator information, and continual improvements to the program to ensure quality information, quality over quantity.

The timeliness of cyber threat information sharing has been negatively impacted, I believe, by the Government's overclassification of threat data, which is really minimizing the value that AIS can provide to the critical infrastructure community.

The agency that is originating this information is sharing that information with DHS, and they're in charge of the classification or declassification of that information. When DHS has to go back and get the originating source to go through the process of declassifying it, it results in delays. That information many times, the threats associated with that can become obsolete, because of the shifting nature of attacks within the internet.

Alternatively, if the information is scrubbed to remove the Classified status, the resulting information is often so cleansed or minimized that much of the relevant context that's needed to properly action it in my organization is removed.

So some proponents have suggested the timeliness issue could be resolved by increasing the number of cleared individuals in critical infrastructure. However, increased access to Classified information for these individuals provides little actionable data that we can take back into our un-Classified networks for implementation. Any shared data that is still classified at that level can't be actioned on an un-Classified fabric.

To speed up the timeliness of information sharing, we encourage our partners in law enforcement and the intelligence community to work to tear-line more of their reporting, so any actionable information, IOCs, hashes, and other things can be shared expeditiously with critical industry. If information is found in open source, the Government should act quickly to declassify the entire report as rapidly as possible.

Also, the equities review process continues to be a stumbling block toward timely, broader, and more actionable information sharing from the Government to private industry. I fully understand the intelligence community must consider both public benefit and operational risk when disclosing confidential information about a threat. However, in light of the public sector's caution when it comes to sharing information about cyber incidents, private industry is instead turning to cybersecurity firms for timelier and more contextually complete information.

At American Express, we rely primarily on FS–ISAC and other sources, both external as well as communities of interest, for a lot of our threat data. We engage in outbound sharing, primarily with FS–ISAC and other financial institution partners, through auto sharing of IOCs and other freeform communication.

Much of the threat information sharing is still being primarily shared via email, as it allows for communication with important context, which includes things of who saw it, what was seen, when was it seen, where, which part of the network, as well as how it was mitigated or contained. This relevant information a lot of times can't be shared in some of these machine-to-machine systems.

Today, the AIS program does not offer this type of valuable context for the indicators that are being shared. Just as the context is important for security analysts, the lack of the context prevents users of the information from confirming that these indicators have been properly vetted as well as received from trustworthy sources.

Additionally, private-sector organizations have shared feedback with DHS that they would like to see a higher volume of contextually rich data versus just a larger volume of less insightful information.

One way DHS can address some of these issues is through the adoption of technology that automates the ability to apply confidence levels by source to the indicator-sharing process. DHS should also consider working more closely with information recipients to learn what kinds of data and context are going to be most useful and pertinent to private industry for our own networks.

Since CISA's passage, public-private information sharing has come a long way and many positive advancements have occurred. We strongly believe that a timelier, more contextual, higher-quality information-sharing program is the next step in the evolution of cyber threat information for DHS.

I want to thank you for inviting me to be here today to discuss this very important issue, and I look forward to answering any questions you may have.

[The prepared statement of Ms. Barron-Dicamillo follows:]

PREPARED STATEMENT OF ANN BARRON-DICAMILLO

NOVEMBER 15, 2017

Chairman Ratcliffe, Ranking Member Richmond, Members of the subcommittee, my name is Ann Barron-Dicamillo, and I am vice president of cyber intelligence and incident response at American Express. Thank you for the opportunity to be here with you today. In my role at American Express, I'm responsible for managing cybersecurity operations and directing cyber threat intelligence globally for the company. I oversee an organization responsible for information security monitoring, security incident response, advanced cyber analytics as well as forensics and other applicable investigations. My organization is on the front lines of defense against active cyber threats, and we actively participate in information sharing with industry and Government partners. As an experienced information security executive with almost 20 years of extensive experience in operations and in the delivery of information security services, I have gained a deep knowledge of the cyber threat intelligence environment and a respected track record of assisting organizations make balanced and informed risk decisions.

From January 2013 to February 2016, I was director of the United States Computer Emergency Readiness Team (US–CERT) at the Department of Homeland Security (DHS). My responsibilities included leading cybersecurity incident-response activities and network analysis, working to share relevant data with both the public and private sectors on cyber threat information-sharing initiatives. At US–CERT, I supported DHS's efforts to improve the Nation's cybersecurity posture, and I directly coordinated cyber information sharing to proactively manage cyber risks. My responsibilities also included driving the US–CERT mission with CERTs around the world, overseeing the 24x7 operations center, analyzing and reducing cyber threats and vulnerabilities, disseminating cyber-threat warning information and supporting incident-response activities with Government and critical industry partners.

I've been a vocal proponent of Cyber Threat Intelligence (CTI) information sharing throughout my career in both my public- and private-sector roles. The fundamental importance of CTI information sharing comes down to one simple concept: "One entity's detection could be another entity's prevention." As computer network defenders, information sharing becomes the foundation upon which we can build a robust cybersecurity program in the continual fight to thwart cyber criminals and other adversaries. CTI information sharing happens even before first-line defenders are engaged; it enables security operation analysts and hunters to be proactive in the search for malicious activities; and it gains us a broader perspective on the threat environment as it perpetuates across the web.

While at DHS, I engaged in efforts to mature public/private CTI information-sharing programs like those created by the Cybersecurity Information Sharing Act of 2015 (CISA). This legislation addressed many of the concerns that had been expressed by critical infrastructure sector partners, including American Express, in engaging in CTI information sharing with the Government. It created the ability for DHS to establish machine-speed sharing while protecting enterprises from associated liability concerns. American Express' support and position on this issue is one of the many reasons I joined their cyber operations team, as it was clear that Amer-

ican Express understood the importance of cyber threat information sharing for the betterment of our public and private partners, both domestically and abroad.

Since the passage of CISA, American Express has developed a more formal standard for sharing cyber threat information. We have engaged in more consistent sharing with the Financial Services Information Sharing and Analysis Center (FS–ISAC). We deployed and have matured a Threat Intelligence Platform (TIP), which currently ingests, on-average, hundreds of thousands of unique threat indicators per month. Our TIP is used by my organization to proactively search for threats, both emerging as well as trending, in the "Wild West" of the internet for potential relevancy to our unique environment. The information we receive from the TIP includes indicators from the FS–ISAC. These indicators of compromise (IOCs) include those shared by the U.S. Government through DHS's Cyber Information Sharing and Collaboration Platform (CISCP).

American Express is not a current participant in DHS's Automated Indicator Sharing (AIS) program. I understand the AIS bi-directional sharing program, to date, has had limited adoption and early challenges in demonstrating its full potential value. While AIS may be a good program for new entrants in cyber information sharing and a good start down the path of private/public sector information sharing, the program would be more effective at protecting organizations from cyber threats if it offered timelier indicator sharing, richer context around the indicator information, and continual improvements to ensure quality information. The following goes into greater detail regarding these points.

IMPROVE TIMELINESS OF INFORMATION SHARING

An issue that minimizes the potential value of the AIS portal information is that the agency that originated the information or indicator is in charge of the classification or declassification of that information. If the information provided is categorized as Classified, the need to go through the process of declassification results in delays in DHS's information-sharing process, making the details of threats quickly obsolete because of the quickly shifting nature of attacks. Alternatively, if the information is scrubbed of its Classified status, the resulting shared information is often so cleansed or minimized that much of the relevant context needed to properly action the information has been removed.

Some proponents have suggested that the timeliness issue can be resolved by increasing the numbers of—and expediting the process to clear—private-sector individuals at companies, so as to be able to get access to Classified information. However, increased access to Classified information by critical infrastructure personnel provides little actionable data for those individuals to take back to their Unclassified networks for implementation, as the data is still Classified at a level that can't be removed or actioned on an Unclassified fabric.

When I was at DHS, to try to help address the classification issue, I encouraged my partners in law enforcement and intelligence to work to "tear-line" more of their reporting so any actionable information could be shared more expeditiously with critical industry stakeholders. (Tear-lining is the process of sanitizing Classified information below the tear line to convey the substance of the information without any identifying or sensitive sources or methods.) If relevant context is getting lost through the tear-line process, then the Government should act to declassify the entire report as rapidly as possible.

In addition, the equities review process continues to be a stumbling block toward broader, more actionable information sharing from the Government to private industry, and over-classification of entire reports continues to be an issue across the board in the intelligence community in all kinds of different contexts. In some instances, the usefulness of the information is essentially eliminated if the context is removed or if the limited information around the threat is misleading, leaving the private sector with a clue of a threat but not the ability to take meaningful, intentional steps to protect its network against an existing threat.

Having worked in these circles responding to cyber events while in the public sector, I fully understand the intelligence community must consider both public benefit and operational risks when disclosing confidential information about a threat. However, in light of the public sector's caution when it comes to cyber incidents, private industry turns to private cybersecurity firms for timelier and contextually complete information.

DHS can best address timeliness of cyber information sharing by working with the originating agency of the information to expedite the equities review process. Alternatively, DHS could work toward tear-lining the reporting, or better yet, if the information is found in an open source, work toward declassifying the reporting.

PROVIDE CONTEXT FOR EFFECTIVE THREAT MITIGATION

At American Express, we rely primarily on the FS–ISAC and other sources of external threat data from vendors and other communities of interest. We engage in outbound sharing primarily with the FS–ISAC and other financial institution partners. Threat sharing within the FS–ISAC occurs in two distinct ways: (1) The automated sharing of indicators via STIX (Structured Threat Information eXpression) and TAXII (Trusted Automated eXchange of Indicator Information); and (2) the sharing of unstructured, free-form emails that describe threats and provide context, including various indicators, and that are exchanged between different trust communities vetted by existing members for operational experience. The bulk of threat information sharing is still primarily via email, since it allows for communication of important context, including who saw it (e.g., sector-specific or wide-spread), what was seen (e.g., specific exploit to a known vulnerability or software version), when it was seen (e.g., when the activity began), where (e.g., impact to specific operating system endpoints or servers or hardware components) or on which part of the network it was seen (e.g., cloud-based, traditional network, or mobile), and how it was mitigated or contained as relevant (e.g., whether there is a patch available or known signatures or scripts to mitigate the exploit ahead of the patch). These are the important details security analysts need in order to identify which indicators are the most relevant and important in their own networks, and how they relate to specific on-going attack campaigns.

Today, the AIS program does not offer this type of valuable context for the indicators that are being shared. Just as the context is important to security analysts, the lack of context prevents users of the information from confirming that the indicators have been properly vetted and received from trustworthy sources. Providing mechanisms for representing and encouraging the supply of additional context, providing real-time feedback on data quality, and supporting different communities of trust are ways to advance the program. Additionally, private-sector organizations, like American Express, have shared feedback with DHS that they would like to see a higher volume of Unclassified sharing versus a larger volume of less insightful information.

There are on-going collaborative developments in information sharing, both in the formation and evolution of information-sharing groups (ISACs, ISAOs, and other formal and informal threat-sharing communities) and in mechanisms for describing and sharing threat information. There are also efforts to make that threat information actionable by defensive measures, such as STIX and TAXII, the MITRE CAPEC (Common Attack Pattern and Classification) and ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge), and the newly-developing OpenC2 (Open Command and Control) standard. The implementation of STIX 2.0, which allows for representation of greater context and the identification of relationships between shared data, would be a beneficial step for AIS.

CONTINUALLY IMPROVE TO ENSURE QUALITY AND TRUSTWORTHINESS OF INFORMATION

DHS should focus on ways to continually assess and improve the quality of the information-sharing process through adoption of technology that automates the ability to apply confidence levels by source to the indicator-sharing process. DHS should consider working more closely with information recipients to learn what data and context are useful and pertinent to private industry so that private industry can easily ingest relevant information in real time. In addition, DHS should work with the private sector to gain confidence in the validity and credibility of the information (through the context sharing described above) while ensuring that the voluntary reporting of threats to the AIS program does not lead to attribution of any particular industry or entity.

Since CISA's passage, private- and public-sector sharing has come a long way and has made many positive advancements, but we believe there is more work to be done to overcome our adversaries. We strongly believe that timelier, more contextual and higher-quality information sharing is the next step in the evolution of cyber threat information sharing that will lead to increased private-sector participation in DHS's information-sharing programs.

I want to thank you again for inviting me to be here today to discuss this very important issue, and I look forward to answering any questions you may have.

Mr. RATCLIFFE. Thank you, Ms. Barron-Dicamillo.

I would now like to recognize Ms. Cagliostro.

Am I saying that right?

Ms. CAGLIOSTRO. Yes, that is correct.

Mr. RATCLIFFE. You're recognized for 5 minutes.

STATEMENT OF PATRICIA CAGLIOSTRO, FEDERAL SOLUTIONS ARCHITECT MANAGER, ANOMALI

Ms. CAGLIOSTRO. Thank you. Thank you, Chairman Ratcliffe, Ranking Member Langevin, and distinguished Members. I'm honored to appear before the committee today to discuss how we can improve the partnership between public and private sector to strengthen our Nation's security with cyber threat information sharing.

I work for a leader in the cyber threat intelligence space called Anomali. We were the first company to automatically share intelligence back to AIS. We also integrate AIS with our technology and provide access to our customer base.

Our deep integration with AIS and experience with facilitating sharing with ISACs and ISAOs provide unique insights into the critical factors for successful sharing programs and opportunities for improvement in the AIS program.

In 2017, the Ponemon Institute commissioned a report that represented over 1,000 organizations from North America and the United Kingdom. This report provides critical insights about the threat intelligence industry that impact the adoption and participation in AIS.

One of the biggest challenges identified by 70 percent of respondents was the volume of data available. To put this in perspective, there are hundreds of millions of indicators from hundreds of sources in the Anomali platform, and we've continued to see the volume of threat data grow exponentially since our inception. AIS is one of many sources that organizations have access to.

The biggest value of threat intelligence is the ability to integrate with an organization's security controls to detect and prevent malicious activity on the network. Think of threat intelligence like the no-fly list that airlines use to prevent threats from flying. If the data wasn't integrated with airline systems, the value of the list would be diminished because it couldn't prevent high-risk passengers from flying.

Threat intelligence is the cyber no-fly list, and when organizations integrate with their security controls, they can actively detect and prevent threats on the network.

Once an organization can consume and integrate threat intelligence, they've reached a maturity level where they're ready to actually share intelligence. Sixty-two percent of organizations reported that they share intelligence today. About 50 percent of those said they share with just the security vendors, while only 30 percent actually share with the Government.

When we think about maximizing the value of information sharing in the context of AIS, we need to keep in mind the state of threat intelligence. Organizations in both the public and private sector need tools to manage and integrate the overwhelming amount of threat intelligence before they're ready to share. When they are ready to share, trust and ease of use are critical for success.

DHS should be commended for meeting the aggressive time lines outlined in the Cybersecurity Act of 2015, but with any large pro-

gram there are always opportunities to improve. The primary goal should be to expand AIS participation to as many organizations as possible because more participants will ultimately impact the quality and improve the quality of the data shared.

DHS can reduce the level of effort for organizations to participate in AIS by increasing the ways that people can access it and integrating it with analyst workflows. When an organization wants to connect to AIS, it can take weeks between legal reviews, between deploying technology for them to actually get connected. DHS should continue to work with third parties who can redistribute AIS through their sharing platform, like ISACs and ISAOs, and security vendors like Anomali, so organizations don't have to add additional technology in order to participate.

Analysts collect and produce cyber intelligence as part of their daily workflow. In the Anomali platform, analysts simply check a box to automatically share with their community. They're more likely to share because it's easy. It doesn't add additional work for them. It's something they would have to do anyway as part of their regular workflow.

The AIS program will benefit by integrating with security technologies like Anomali to make it easier for organizations to share back, so, again, as part of that daily workflow.

Cybersecurity isn't a marathon or a sprint. There is no finish line in sight. We face a dynamic adversary, and we need to use every advantage that we have. The attack surface is too large and resources are stretched too thin for organizations to defend alone. Information sharing acts as a force multiplier and can help level the playing field.

In the most recent election, the Colorado State ISAC partnered with Anomali to share intelligence in real time with various Federal, State, and local organizations to maximize their ability to defend the integrity of our elections.

Real-world success stories of the power of information sharing, supported by public and private-sector partnerships, will continue to drive adoption and participation in programs like AIS.

Thank you guys for inviting me today.

[The prepared statement of Ms. Cagliostro follows:]

PREPARED STATEMENT OF PATRICIA CAGLIOSTRO

NOVEMBER 15, 2017

Chairman Ratcliffe, Ranking Member Richmond, and distinguished Members, I am honored to appear before the committees today to discuss how we can improve the partnership between the public and private sector to improve our Nation's security with cyber threat information sharing.

I work for a leader in the cyber threat intelligence space called Anomali. At Anomali, we have worked closely with the public and the private sector to enable information sharing for several years. My role is to lead a team of professionals in the global public sector to solve the biggest challenges in leveraging threat intelligence to stop critical threats and facilitate relationships between industry and the public sector.

Anomali was the first company to automatically share intelligence back to the Department of Homeland Security's Automated Indicator Sharing program, referred to as AIS. We also integrate AIS information with our technology and provide access to approved customers. Our deep integration with AIS and experience with facilitating cyber intelligence-sharing communities provides unique insights into the critical factors for successful sharing programs and opportunities for improvement in the AIS program.

In my testimony, I will describe the state of threat intelligence in the private sector, how we can reduce the barrier to entry for the private sector to share information through AIS and improve the quality of information provided by AIS.

STATE OF THREAT INTELLIGENCE

In 2017, the Ponemon Institute commissioned a report: The Value of Threat Intelligence: A Study of North American and United Kingdom Companies that included over 1,000 respondents. (*https://www.anomali.com/resources/whitepapers/value-of-threat-intelligence-ponemon-study*) This report provides valuable insight into how the private sector uses and consumes threat intelligence. The report found that 80% of organizations use threat intelligence and of those organizations, 84% identified threat intelligence as essential to a strong security posture.

One of the biggest challenges identified by 70% of respondents was the volume of available threat data. Today, there are over 400 million indicators of compromise in the Anomali platform and we have seen the volume of threat data from open, shared intelligence and threat intelligence vendors grow exponentially since our inception. Threat Intelligence Platforms like Anomali enable organizations to aggregate and consume the overwhelming amount of threat intelligence available to organizations.

The biggest value of threat intelligence is the ability to integrate with an organization's security controls to detect and prevent malicious activity on the network. 65% of respondents cited integration as necessary to maximize the value of threat intelligence data. Think of the No-Fly List that airlines use to prevent threats from flying. If the data wasn't integrated with airline and airport security systems, the value of the list would be diminished because it couldn't prevent high-risk passengers from flying. Threat intelligence integration provides the cyber no-fly list by integrating with security controls to detect and prevent threats.

Once an organization can consume and integrate threat intelligence, they have reached a maturity level where they are ready to share intelligence. Sixty-two percent of organizations reported that they share intelligence. Of those organizations, 50% share with trusted security vendors and 43% share with trusted peer groups while only 30% of organizations reported sharing with the government through programs like AIS and CISCP. Organizations identified a lack of threat intelligence expertise as the primary reason why they do not share intelligence.

When we think about maximizing the value of information sharing in the context of AIS, we need to keep in mind the state of threat intelligence in the private sector. In my experience, these challenges are also relevant in the public sector. You have to help yourself before you help others and organizations in both the public and private sector need the tools to handle the overwhelming amount of threat data and integrate the intelligence before they are ready to share intelligence. When they are ready to share, trust and ease of use are critical for success.

BARRIERS TO ENTRY FOR PRIVATE INDUSTRY

The barrier to information sharing through AIS and the quality of information provided by AIS are intimately related because a significant portion of the information provided by AIS is shared by the participants. If participants do not share valuable information through AIS, the quality of the information that is delivered will be impacted. The level of effort to share intelligence through AIS and lack of expertise in threat intelligence act as barriers to entry to share intelligence through AIS.

When an organization wants to connect to AIS, they must sign a terms of use document, setup a TAXII client, purchase a PKI certificate from a commercial provider, provide your IP address to DHS and sign an Interconnection Security Agreement. While this may not seem overly complex, this process can take private organizations weeks to complete because of legal reviews and change control processes. In the public sector, this can be even more time-consuming because additional processes and requirements can cause delays due to the time to get new technologies on-line.

Once an organization is connected to AIS, they often find it difficult to share intelligence. While there are a variety of options available to private industry to share with AIS including TAXII client software, a DHS website and email, they add additional work for analysts outside of their workflow. Almost every organization is struggling with the resource shortage in cybersecurity, and adding additional work to share information will negatively impact participation rates.

There is an extremely limited supply of skilled threat intelligence analysts. When organizations share intelligence, they may be concerned that they do not have the expertise to produce relevant intelligence that other organizations will find useful. Organizations are afraid to be the boy who cried wolf and look immature for sharing intelligence that other organizations will not find useful.

These challenges are common for any information-sharing program and are the first hurdle that Information Sharing Analysis Organizations and Centers or ISACs and ISAOs must overcome. Anomali is the technology platform for several ISACs and ISAOs and has identified several solutions to reduce the barrier to entry for organizations to share that can be applied to AIS.

When a new ISAC or ISAO partners with Anomali, the time line for their members to gain access and start contributing is extremely short. ISACs and ISAOs are provided with their own instance of the solution and the members are automatically added to the platform. They simply login to begin collaborating rather than waiting to deploy technology in their own environment. We also work with the ISACs and ISAOs to provide member outreach and deliver training so companies feel comfortable with the solution. There is data already present in their instance from open source and the ISAC which provides immediate value to the analyst. The AIS program would benefit from continuing to partner with third-party organizations like ISACs and ISAOs an security vendors like Anomali to streamline the process to gain access to AIS.

Analysts collect and produce cyber threat intelligence as part of their daily workflow. In the Anomali platform, analysts simply check a box to automatically share intelligence with their community. They are more likely to share because it's integrated with their daily workflows, rather than an additional step or technology they must work with. The AIS program will benefit from outreach by DHS to the security industry to further integrate sharing with the technologies that analysts use every day.

Analysts on the Anomali platform have a variety of options to contribute that range from providing net new intelligence to enriching existing intelligence. Analysts benefit from the diversity in sharing mechanisms because they can participate at the level they feel comfortable. Not all organizations produce net new intelligence and allowing analysts to enrich existing intelligence with data like sightings on their network or associations to an actor makes sharing less intimidating and reduces the level of experience an analyst needs to participate. The AIS program can benefit by expanding the types of intelligence analysts can share beyond just indicators of compromise.

QUALITY OF INTELLIGENCE

Measuring the quality of cyber intelligence can be incredibly difficult because the value will vary based on who the organization is and how they use threat intelligence. At Anomali, we work closely with our customer base to more intimately understand what factors impact the quality of intelligence they are leveraging. Ultimately, when discussing the quality of intelligence, organizations want relevant intelligence. They want to understand out of the millions of indicators that are available, which ones need their attention. Relevant intelligence is extremely powerful because it helps drive response and reduce time wasted on low-priority information.

Think of cyber intelligence like a weather report. If I told you it was going to be 65 degrees, would you wear a jacket? Before you made your decision, you would want to know contextual details like where did I get the report from, has my source been accurate in the past, and when and where it was going to be that temperature. If I am a trusted source, you may just take my word for it because I know what makes the report relevant to you. If I knew that it is going to be 65 degrees, I would wear t-shirt and shorts. If you are like my college roommate from California, it's time for the down jacket.

Like the weather example, organizations derive relevance from context about intelligence and the organization's own requirements to make decisions. The more context they have about shared intelligence, the easier it becomes to determine if it's relevant and select a course of action. In the Anomali platform we enrich threat intelligence with the contextual data and provide the tools that organizations need to easily identify relevant intelligence. Our data model has defined threat intelligence objects supported by flexible fields that allows organizations to capture and store additional types of contextual data.

Today, AIS information has limited context which impacts the private sector's ability to determine relevance and determine the appropriate course of action. Organizations look at factors like the source, confidence level, impact type, timeliness, and sightings among other factors to determine relevance. The next iteration of AIS supports STIX 2.0 which expands the AIS schema to allow for more context which will improve the quality of the AIS data.

CONCLUSION

When I first started at Anomali, people often asked how we forced people to share intelligence. People assumed that when we talked about sharing, we had to be forcing people because no one would choose share unless they had to. Our approach wasn't to force people to share, but to create an environment where sharing was easy and organizations received value.

The AIS program has come a long way since its inception and as the barriers to entry are reduced, more organizations will participate and increase the quality of the data provided.

Mr. RATCLIFFE. Thank you, Ms. Cagliostro.

Mr. Mayer, you are recognized for 5 minutes.

STATEMENT OF ROBERT H. MAYER, SENIOR VICE PRESIDENT FOR CYBERSECURITY, US TELECOM ASSOCIATION

Mr. MAYER. Chairman Ratcliffe, Ranking Member Langevin, and Members of the subcommittee, thank you for the opportunity to appear before you today for this important hearing.

My name is Robert Mayer, and I serve as senior vice president for cybersecurity at USTelecom. I also serve as chair of the Communications Sector Coordinating Council, which represents the broadcast, cable, satellite, wireless, and wireline segments of the communications industry. The CSCC is one of 16 critical infrastructure sectors operating through the Department of Homeland Security's Critical Infrastructure Partnership Advisory Council.

Today the wide variety and large volume of cyber threat information sources, along with the growing number of information-sharing venues, presents both opportunities and challenges in creating real value to information sharing.

Since the passage of the Cybersecurity Information Sharing Act of 2015, much has been done to reduce obstacles to sharing and to facilitate enabling mechanisms and venues. The communications sector works on multiple fronts to share cyber threat information. In my written testimony, I note that for more than 35 years, dating back to the Cold War era, the U.S. Government has worked in operational partnership with the communications sector to better assure the reliability, availability, and resiliency of our networks.

The relationship between the communications sector and the DHS National Coordinating Center for Communication stands alone among critical infrastructure information-sharing partnerships in both depth and length of partnership.

Jointly, the relationship between the Communications Sector Information Sharing and Analysis Center, the Comm–ISAC, with over 65 participating private-sector companies, and the NCC, is one that many sectors are attempting to replicate.

Five of the largest domestic network service providers have representatives embedded within the NCC and through the NCC work on the floor of the National Cybersecurity Communications Integration Center, or NCCIC, as it is known.

Many more formal and informal structured and unstructured venues are described in the March 2017 FCC CSRIC report referenced in my testimony.

As a practical matter, companies will participate in information-sharing activities to the extent that they perceive the benefits outweigh or at least match the costs. Any information-sharing venue and mechanism that does not provide contextualized, timely, accu-

rate, and actionable information that improves the provider's security posture will not meet the test.

The CSRIC report found that a critical organizational challenge facing our sector is the wide variety of private, public, public-to-private, and international activities devoted to cyber information sharing.

Many organizations, especially smaller service providers, are unfamiliar with the breadth and depth of information-sharing entities or lack the resources to commit to these enterprises. These organizations are in most cases unable to devote scarce resources to time-consuming efforts to filter numerous sources of threat intelligence, validate what is applicable, and then set implementation priorities.

While there are no easy solutions for these companies, trade associations, like USTelecom, and the 13 other sector trade associations that are also members of the CSCC provide a critical link to information resources that can enhance their security posture.

For many of the larger service providers, the distribution of Classified information from the Federal Government is an essential element of their overall risk-management capabilities, and this can impact the quality of information shared between private parties and within organizations.

We continue to request Classified information when available, and we also ask that those pieces be downgraded as much as possible so that dissemination to the practitioners in the field can take place quickly.

With respect to the DHS AIS portal, there is still important work that needs to be done to increase the value proposition for companies within our sector. Most of the concerns with AIS relate to the quality and usability of the information for the particular needs of an ISP and its enterprise. While the information distributed via AIS may be helpful to certain entities, the value proposition remains elusive for companies with more mature, sophisticated cybersecurity programs.

To make cyber threat information sharing more viable and valuable, we encourage the Government to look across various information-sharing programs and analyze whether they are functioning as intended, meeting the needs of their target audiences, and identify gaps that need to be filled. Doing this will ultimately result in higher quality, contextualized, and more timely information being shared.

The good news is that DHS is aware of the current limitations and is committed publicly to a multi-year effort to enhance the automated machine-to-machine sharing capabilities. DHS is to be applauded for its on-going and accelerating outreach efforts to engage industry and to increase the value of their information-sharing programs.

We remain committed to bringing all available industry resources to bear in this vital area, and I look forward to answering any of your questions. Thank you.

[The prepared statement of Mr. Mayer follows:]

PREPARED STATEMENT OF ROBERT H. MAYER

NOVEMBER 15, 2017

Chairman Ratcliffe, Ranking Member Richmond, and distinguished Members of the subcommittee, thank you for giving the communications sector and me personally the opportunity to appear before you today for this important hearing on maximizing the value of cyber threat information sharing.

My name is Robert Mayer, and I serve as senior vice president cybersecurity at USTelecom which represents companies ranging from some of the smallest rural broadband providers to some of the largest companies in the U.S. economy. I also serve as chair of the Communications Sector Coordinating Council (CSCC) which represents the broadcast, cable, satellite, wireless, and wireline segments of the communications industry.[1] The CSCC is one of the 16 critical infrastructure sectors under the Critical Infrastructure Partnership Advisory Council (CIPAC) through which the Department of Homeland Security (DHS) facilitates physical and cyber coordination and planning activities among the private sector and Federal, State, local, territorial, and Tribal governments.

I want to thank the Members of this subcommittee for emphasizing the concept of value in the context of information sharing. Of course, we endeavor to share cyber threat information not for information sharing's sake, but for the purpose of adding value to our operational and strategic cyber preparedness and defense efforts.

Today, the wide variety and large volume of cyber threat information sources, along with the growing number of information-sharing venues, presents both opportunities and challenges in creating real value to information sharing. Since the passage of the Cybersecurity Information Sharing Act of 2015,[2] much has been done to reduce obstacles to sharing and to facilitate enabling mechanisms and venues. Still, this law is just the statutory foundation that will enable the actual sharing processes that need to be implemented; getting the right information to the right people at the right time with the appropriate privacy and security safeguards. This massive effort requires constant innovation, on-going evaluation and disciplined resource allocation. Below I briefly outline the work of our sector in this area, some on-going challenges, and the important role of the DHS as a facilitator of cybersecurity information sharing.

The Communications Sector works on multiple fronts to share cyber threat information, and individual companies use a variety of information-sharing platforms and services to achieve their objectives. From a sector perspective, two of the most prominent and robust information-sharing venues operate in partnership with DHS.

First, the relationship between the Communications Sector and the DHS National Coordinating Center for Communications (NCC)[3] stands alone among critical infrastructure information-sharing partnerships in both depth and length of partnership. Jointly, the relationship between the Communications Sector Information Sharing and Analysis Center (Comm–ISAC) and the NCC is one that many sectors are attempting to replicate. For more than 35 years, dating back to Cold War era existential concerns about telecommunications reliability and disaster recovery, the U.S. Government has worked in operational partnership with leaders of the communications sector to better assure the reliability, availability, and resiliency of our networks. DHS NCC provides our industry with 24/7 on-site watch desk functions, helps coordinate the communications sector for preparedness and response to both physical and cyber events, and acts as the information exchange portal to Government for us, and likewise as Government's portal to the Communications Sector. The Comm–ISAC includes over 65 private-sector companies that convene weekly, and on an as-needed basis, to share information about events and threats that have or could have adverse impacts on network service providers and their customers.

Second, aligned with NCC activities is the Network Security Information Exchange (NSIE) which meets every 2 months and is comprised of companies that support DHS's and the Communications Sector's National security mission.[4] During these sessions, analysts and security managers discuss threats and other issues that directly implicate the reliability, resiliency, and integrity of the communications environment. Five of the largest domestic network service providers have representatives embedded within the NCC and are on-call to respond to Government inquiries

---

[1] Communications Sector Coordinating Council, *https://www.comms-scc.org*.

[2] Cybersecurity Information Sharing Act of 2015, *https://www.Congress.gov/bill/114th-congress/senate-bill/754*.

[3] National Coordinating Center for Communications, Department of Homeland Security, *https://www.dhs.gov/national-coordinating-center-communications*.

[4] Network Security Information Exchanges, Department of Homeland Security, *https://www.dhs.gov/sites/default/files/publications/NSTAC__08__0.pdf*.

related to infrastructure-impacting events of either a cyber or physical nature. Since the NCC is one of three operational components along with US–CERT and the ICS–CERT on the National Cybersecurity and Communications Integration Center (NCCIC) floor, these same individuals are embedded within the NCCIC.

The NCCIC is a 24/7 cyber situational awareness, incident response, and management center and operates as the principal Federal civilian interface for multi-directional and cross-sector information sharing. Through the auspices of the NCCIC, and more broadly the DHS Office of Cybersecurity & Communications, communications sector companies currently work with the DHS Automated Information Sharing (AIS) portal using the STIX/TAXII protocols, which is designed to facilitate real-time sharing of cyber threat indicators.[5] Many of the largest providers are working through the AIS portal, as well as other related venues, to improve and increase the effectiveness and efficiency of automated sharing for more end-users. Also under the NCCIC, member companies participate in the Cyber Information Sharing and Collaboration Program (CISCP) which provides a collaborative and trusted environment in which analysts from multiple sectors learn from each other to better understand and address emerging cybersecurity risks.[6]

Many more formal and informal venues and sharing mechanisms are described in the March 2017 report on Cybersecurity Information Sharing from the Federal Communications Commission's Communications Security, Reliability, and Interoperability Council (CSRIC) Working Group 5 (CSRIC report).[7] I now wish to touch on some significant findings in that report, as well as general observations about current information-sharing venues and platforms.

First, as a practical matter and returning to the question of value that is the focus of this hearing, companies will participate in information-sharing activities to the extent that they perceive the benefits outweigh, or at least match, the costs. Given the pressures on providers to ensure the confidentiality, integrity, and availability of their communications networks and systems, any information-sharing venue or mechanism that does not produce contextualized, timely, accurate, and actionable information that improves providers' security posture will not meet that test of value.

More broadly, the CSRIC report found that a critical organizational challenge facing the communications sector is the wide variety of private, public, public-to-private, and international activities devoted to cyber threat information sharing.[8] Many organizations, especially smaller service providers, are unfamiliar with the breadth and depth of information-sharing entities or lack the resources to commit to these enterprises. The rapid expansion of information-sharing venues such as the Information Sharing and Analysis Organizations (ISAOs) called for under the 2015 Executive Order "Promoting Private Sector Cybersecurity Information Sharing" threatens to dilute resources and expertise through redundant or conflicting activities and objectives.[9]

For many of the larger service providers, the distribution of Classified information from the Federal Government is an essential element of their overall risk management capabilities and this can impact the quality of information shared between private parties and within organizations. Having access to contextualized and actionable Classified information is highly valuable. Similarly, not having access to such contextual information is detrimental to operations, but so is being unable to share some, or most, of the information with non-cleared colleagues. We continue to request Classified information, when available, and we also ask that those pieces be downgraded as much as possible so that dissemination to the practitioners in the sector can take place quickly.

With respect to the DHS AIS portal, there is still important work that needs to be done to increase the value proposition for companies within our sector. Most of the concerns with AIS relate to the quality and usability of the information for the particular needs of an ISP and its enterprise. AIS is, and was intended to be, a platform for broad, cross-sector sharing that has resulted in information being downgraded or simplified to be appropriate for all participating entities. While the information distributed via AIS may be helpful to certain entities, the value proposition

---

[5] Automated Indicator Sharing (AIS), Department of Homeland Security, *https://www.us-cert.gov/ais*.

[6] Cyber Information Sharing and Collaboration Program (CISCP), Department of Homeland Security, *https://www.dhs.gov/ciscp*.

[7] CSRIC Working Group 5—Final Report, Federal Communications Commission, *https://www.fcc.gov/files/csric5-wg5-finalreport031517pdf*.

[8] Id. at 13.

[9] Executive Order—*Promoting Private Sector Cybersecurity Information Sharing*, The White House—President Barack Obama, *https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari*.

remains elusive for companies with more mature, sophisticated cybersecurity programs.

To make cyber threat information sharing more viable and valuable, we encourage the Government to look across the various information-sharing programs such as AIS and CISCP and analyze whether they are functioning as intended, meeting the needs of their target audiences and identify gaps that need to be filled. For example, the Government needs to take the next step and determine whether there are more effective ways to share information with companies who have more mature programs, and specifically those who have been described as "ICT enablers"—i.e., the ICT companies that provide key services that enable the cyber ecosystem. Doing so will ultimately result in better and more timely information being shared.

I want to be clear that in highlighting current challenges we are working on with Government, I do not mean to suggest that there is not currently valuable information sharing underway. A Comm–ISAC member receives more than one dozen alerts a day through the NCC from NCCIC, US–CERT, ICS–CERT, ISACs, and joint law enforcement bulletins, and one company reports that it can trace the addition of 2,800 unique indicators in the past 10 months from the various DHS sources.

The good news is that DHS is aware of the current limitations and appears to be committed to a multi-year effort to enhance the automated machine-to-machine sharing capabilities. Our industry is committed to this program as evidenced by broad sector participation in a pilot managed by CTIA.[10] That program is about to be operationalized after testing new adaptations of the sharing platform to conform to communications sector operating environments.

Finally, I want to draw attention to the hundreds of smaller companies in our sector who face a different set of challenges due largely to their limited financial resources, technical skill-sets, and operational priorities. These organizations are in most cases unable to devote scarce resources to time-consuming efforts to filter numerous sources of threat intelligence, validate what is applicable, and then set implementation priorities. In many instances, they are unaware of information-sharing venues, especially those venues that are operated by the private sector and accessed via exclusive invitation. While there are no easy solutions for these companies, trade associations like USTelecom and multiple other associations that comprise the CSCC are providing a critical link to information resources that can enhance their security posture.

Despite these and other challenges, and the risk of oversaturating the information-sharing space with low-value activity, I do want to emphasize that without effective information sharing we have no hope of combatting emerging threats to our National and economic security. DHS is to be applauded for its on-going efforts to engage industry and to increase the value of their information-sharing programs. We remain committed to bringing all available industry resources to bear in this vital area, and I look forward to answering any of your questions.

Mr. RATCLIFFE. Thank you, Mr. Mayer.

Thanks again to all of our witnesses for your testimony today.

I now recognize myself for 5 minutes for questions.

Ms. Barron-Dicamillo, I want to start with you, because you've got sort-of unique experience, extensive experience with US–CERT at DHS. Now in the private sector at American Express you have the opportunity to be part of what I think is the gold standard organization with respect to information sharing on the private side, the FS–ISAC.

We can talk about legislation all day, but the one thing that we can't legislate is confidence. So from your perspective, what are the one or two or three things that you would recommend that DHS do or do better, perhaps, to build confidence in the private sector in both the validity and the credibility of cyber threat information that's being shared?

Ms. BARRON-DICAMILLO. So getting back to some of the comments I made in my opening remarks, I think DHS, a lot of times they're not the original source associated with information that

[10] Protecting America's Wireless Networks, CTIA, *https://www.ctia.org/docs/default-source/default-document-library/protecting-americas-wireless-networks.pdf* at 9.

they're sharing. So creating those closer partnerships with the community in which they're receiving information from, some of it comes from vendors and some of it comes from other Government partners.

In doing that, they need to ensure that the message is being carried that methods and sourcing of the—the source of attribution, those aren't important actions for the community to implement within their network.

Really, breaking apart those two things is a focus there, being that—continuing to communicate with their Government partners on the importance of that so that they can create those trusted relationships with private industry.

I think, from my perspective, the confidence is going to come based on the value of the indicators that they share. When those indicators are proved to be unique and different from what we receive from other sources, that increases the confidence that they will get from the larger private industry community.

Mr. RATCLIFFE. Terrific. Thanks very much.

Mr. Knake, before I came to Congress, my colleague Mr. Langevin worked on prior iterations of a bill we were able to successfully get across the finish line in December 2015, the Cybersecurity Act of 2015.

From your perspective, has the passage of that legislation affected the flow of cyber threat information? Have you seen it change? Has the threat landscape that companies and the Government face, has that changed or been affected by our legislation?

Mr. KNAKE. Mr. Chairman, in my view, what's happened is that we've taken away the excuses for not sharing information, but the reality is many companies still want to find an excuse not to share. So you can no longer say: "Oh, we're worried about anti-trust issues, we're worried the FTC is going to come after us, DOJ is going to come after us."

The reality is that for those companies that had those fears before the legislation, the legislation didn't remove that as a barrier in their minds.

So I do think there's a small element of needing to educate general counsels at large corporations on this issue. I spend a lot of time working with leaders in the community, encouraging them to push back when they are told by their lawyers that they cannot share.

But in my view the real issue isn't the barriers to information sharing, it's the incentives for information sharing. You really need to find ways, we need to find ways as a community to encourage companies to want to share, right?

They want to receive indicators all day long, but taking the act of extracting an indicator from their network and pushing it out to DHS is sometimes not worth the effort. In their minds, it does nothing to protect them. That I think is the main reason we haven't seen a flourishing of information sharing.

Mr. RATCLIFFE. So do you have any suggestions for how we further encourage that?

Mr. KNAKE. I mean, I think the basic one I think would be to encourage it ahead of time, before an incident happens. So this is where I look to insurance as a possible incentive. If Government

were to provide a backstop to cyber insurance, that in exchange for lower premiums you obligated your company to participate in this kind of information sharing, that I think is the kind of incentive that we need now to encourage information sharing.

If you said, we have to do this because we're getting a lower rate, sort of like Progressive on your car insurance, right, under that model, I think we could incentivize more information sharing.

Mr. RATCLIFFE. Thanks very much.

Ms. Cagliostro, very quickly. Last week, in a report from the Office of Inspector General on DHS's implementation of the Cybersecurity Act of 2015 it was recommended that in order to achieve their mission DHS should obtain, "the tools and technologies needed to provide a cross-domain solution for sharing and processing cyber threat information between the Classified and Unclassified repositories."

As DHS evaluates potential solutions for this, what are your thoughts about the criteria for success for what those tools can be?

Ms. CAGLIOSTRO. Sure. So when you talk about cyber intelligence, it's a little bit different than traditional human intelligence. In order to go and get access to human intelligence, you have to put resources in country, language. There's a tremendous time and effort resource commitment there.

For cyber threat intelligence, it's a little bit different, because essentially I can deploy technologies and start collecting cyber intelligence, and there's a very low barrier to entry. That's why I think for when you're thinking about cross-domain and bringing intelligence both up and down in both directions, it's important to know at both levels where intelligence is located.

So on the Classified side, for example, if it's already out there in the public domain, then why is it still Classified? Why is that indicator still Classified? The association to an actor, how we discovered it, that might be sensitive, but the indicator itself shouldn't be.

So I think when you're thinking about tools and technologies, one of the big first steps should be aggregating the publicly available information, so that way we can more effectively and more quickly declassify tools.

Then the second piece becomes it needs to be a machine-to-machine process. My background's the Department of Defense. There's a number of ways to handle cross-domain. Some of it is very manual; some of it is automatic. I think it needs to be something that is a machine process. It shouldn't be someone once a day logging in to download files and copy them over.

Mr. RATCLIFFE. Terrific. Very much appreciate the responses.

The Chair now recognizes the gentleman from Rhode Island, Mr. Langevin.

Mr. LANGEVIN. Thank you, Mr. Chairman.

Again, I want to thank all of our witnesses for your testimony today and the work you're doing on this topic.

So if I could, I'd start with Ms. Barron-Dicamillo.

Thank you again for your work at US–CERT and, again, for your testimony here and for, again, your previous Government service.

So it's clear that you've greatly contributed to advancing the cybersecurity of our Nation and that you appreciate the value of in-

formation sharing. However, I would just mention that in your testimony you state that American Express has not participated in the AIS program due to limited adoption and early challenges in demonstrating its full potential value, and that you engage in outbound sharing primarily with the FS–ISAC and other financial institution partners.

So while I recognize that we can do more as a Government to increase the quality of the data that we share, the value of information sharing itself is predicated on all parties actively participating. We need major corporations like American Express to be involved.

So what is your plan for joining this program and contributing the insights that you gain on a daily basis in defending your networks?

Ms. BARRON-DICAMILLO. So through FS–ISAC, we actually participate in the AIS program. We're not a direct participant, but we get the—we share information through FS–ISAC, so we are outbound sharing that information, which is also shared back from FS–ISAC into the AIS community. Then AIS shares it through FS–ISAC back to financial institutions like us. So we do benefit from it through that relationship we have with FS–ISAC.

The reason why we haven't joined specifically is associated with the CRADA agreement that you must sign when you join these programs at Homeland Security. In doing so, it precludes us from bringing on any additional cleared individuals within American Express, because you have to go through a private industry—or you have to go through the DOD private industry clearance process. When you have a CRADA agreement with DHS, you are forced through the facility clearance process versus the DOD clearance process for individuals.

So we are not interested in creating infrastructure through the facility clearance process, and that's primarily the reason why we don't have the direct CRADA agreement with Homeland Security for CISCP or AIS.

Mr. LANGEVIN. So is that something that—a policy change between the company and DHS that needs to change?

Ms. BARRON-DICAMILLO. It's probably a policy change between Homeland Security and DOD.

Mr. LANGEVIN. OK. Well, that's something that we can look at. Thank you.

Ms. BARRON-DICAMILLO. I'm not the only financial institution that has that perspective. It would preclude any other critical infrastructure participant from engaging in those programs when they sign the CRADA, or engage in getting additional cleared individuals through the clearance process when they sign that CRADA.

Mr. LANGEVIN. OK. Thank you very much for that insight.

So I thank the Chairman for the question that he asked, the second question, really what's changed. He asked Mr. Knake. So I'd like to give the opportunity to you, Ms. Barron-Dicamillo and Mr. Mayer.

The Cybersecurity Act of 2015, again, made substantial changes to the legal authorities regarding cyber threat indicator sharing. So what are your organizations or, for you and Mr. Mayer, your member companies doing differently today thanks to those authorities and liability protections?

I guess as a follow-up I could say, were any of those actions impermissible before the law and what changed the calculus in your organization?

Mr. MAYER. Thank you, Congressman.

I do think that the act had some significant benefits. I mean, if nothing else, it created awareness on the part of our member companies that information sharing was something that was available, and it took care of some of the liability concerns we had about sharing threat indicators.

I would put it in the category of saying that the act was necessary, but it's not necessarily sufficient to incentivize all companies to participate.

I think for our members who are more mature who have the resources around cybersecurity, for them a lot of the information they get from private sources, as well as their ability to track global network flows and do their own analysis around anomalies and things like that, it's faster, it's contextualized. It limits the incentive to participate in some of the information-sharing venues that currently exist.

Having said that, I would say that there's no shortage of information-sharing activities that are underway in our sector. We have identified informal, formal, structured, and unstructured venues where information sharing is currently taking place. It's a very active community.

Mr. LANGEVIN. But I just want to know, really, what's changed? What more specific things have changed since the act was passed?

Mr. MAYER. Well, I think people have become more aware of the need to share information, and there's a greater willingness to do that. I think what I see is that the information-sharing venues that exist are more robust today.

Our association, for example, has recently created an information-sharing mechanism for small and mid-size businesses. What we've heard from them is they don't have the resources to participate in all of the information-sharing venues. They appreciate a central association helping them in terms of setting priorities and where to look for information.

But we have to go by—we have to understand that each company is going to make their own determination about the value of participating in information sharing. There's no one-size-fits-all here.

So the answer to your question is, directionally, we've made progress in information sharing. I don't know how to tell you that it's correlated directly to the Information Sharing Act.

Mr. LANGEVIN. OK. Thank you, Mr. Mayer.

Ms. Barron-Dicamillo.

Ms. BARRON-DICAMILLO. I concur with the comments from Mr. Mayer. I think we've seen increased visibility associated with information-sharing organizations. There's been an increased participation beyond just the ISACs, so all different types of communities being able to engage in this, and those communities then engaging back with the Government.

So the increased visibility across industry from the passage of CISA and I think the aspect of liability protection has also encouraged many to engage in ISAOs, ISACs, and others, which is that bridge toward information sharing with the Government.

Mr. LANGEVIN. Thank you very much. I yield back.

Mr. RATCLIFFE. I thank the gentleman.

The Chair now recognizes the gentleman from New York, Mr. Donovan.

Mr. DONOVAN. Thank you, Mr. Chairman.

I preface this with all of our cyber hearings by you're talking to a guy whose VCR still blinks 12. So you have to speak to me in layman's terms.

I guess the Chairman's goal here is to find out incentives for information sharing. I guess the first thing you have to look at is, like, what's the disincentives?

So maybe all of you could just explain to me what the disincentives are. As a layperson, I would think that maybe you wouldn't want your competitors to know of your vulnerabilities. Maybe there's a fiduciary duty with your clients that if your data is vulnerable that that might be a disincentive of alerting the world that there's vulnerabilities in the system.

So maybe you just could explain to me what the disincentives are for information sharing or exposures or attempts of attacks for each of you, and then maybe we could talk about the incentives.

Your National Transportation Safety Board, for somebody who is not as familiar as you are, sounds like a wonderful idea. But maybe we could talk about the disincentives first. Can you explain to me a little bit about that and then we can figure out how to give incentives for people to do it?

Mr. KNAKE. Thank you, Congressman.

I would break the disincentives up into two categories. One would be reputational risk. If I'm saying, we've been targeted, somebody's penetrated through our network, they're inside, we found them there, here are the indicators that you can use to see if they're inside your network, that can introduce reputational risk. That could cause problems for stock. That could cause problems with regulators.

The protections that were put in place I think address many of those concerns, to the extent they can be addressed through legislation, but there are things that are outside the control of that legislation.

The other factor I would say is the work factor. If I'm as an organization going to share information with another organization, that's going to require me to do work. That's going for me to require that I take staff and give them the responsibility of sharing the information that other companies want. If I'm in the situation in which my network has been compromised, the last thing I'm thinking about is her network.

So I think that those are the two things that keep companies from sharing information.

Ms. BARRON-DICAMILLO. I concur with Rob's remarks. I definitely agree that reputational risk associated with information sharing is paramount. It's in the front of your mind when you're doing this. A lot of times you're ensuring that the source of information is not to be attributed.

We leverage the traffic light protocol so that we can, as we're sharing information, we can tell the recipient, is this something that you can share publicly, or is this something you can share

within your community, or is this something that is only between me and you as an individual.

That's been really helpful for addressing the reputational risk associated with that. Then you understand where that information is going to go on the other side.

Again, that is through a trusted relationship. So you have to have a trusted community in which you can share that information that adheres to those stipulations associated with the TLP.

Then I definitely agree with the overhead to sharing. You have to have a robust program in place, because as you share information, you're going to get questions back. You want to make sure you have the resources to provide that potential context that might be needed for their individual environment.

So there's definitely going to be—you're going to have to have the maturity within your organization to be able to—the resources to be able to share that information in a way that it doesn't cause them more work on the other end, and then trying to figure out how to implement things, which can sometimes happen and cause, you know, the lack of sharing.

Mr. DONOVAN. Ms. Cagliostro.

Ms. CAGLIOSTRO. I think there's two big reasons why people aren't sharing. I think the first is, is this kind of lack of expertise, especially in the small and mid-size market, where they don't feel comfortable. Maybe they don't know if something is going to be relevant to everyone else. There's insecurity, and you don't want to be the organization that's sharing irrelevant intelligence.

When you think about some of the large organizations, they have full threat intelligence teams, they're producing intelligence, and so there's a lot more that they can share.

For an organization that's a small or medium business, it might be as simple as they've seen this on their network.

That can be useful information to other organizations as well. If you're in the financial services vertical and a ton of small banks are seeing a—you know, they're all seeing the same indicator, they don't need to share net new intelligence, but telling the other banks that they're seeing that is useful information.

I also think that it's got to be really easy for people to share. We talk all the time about how often we don't have enough resource in cybersecurity and analysts are overburdened. No one in cybersecurity says, "Man, I have way too much free time, I wish I had more things to do."

So when we think about sharing, it has to be something that is really easy for them. Like for Amex, for example, they're part of FS–ISAC. They're already sharing with organizations. What do they need to do? Why should they share with the Government? Why should they add this additional step in their processes?

So I think when we're talking about how we can improve for AIS in particular and incentivize sharing, I think the first is to make it easy for people to do. They shouldn't have to stand up additional technology. They shouldn't have to go—it shouldn't be a separate workflow for them. It should be part of what they're doing already.

I think the other side is that what's unique about the Government is that you have unprecedented visibility and unprecedented—unmatched visibility, rather. If I'm explaining to my exec-

utive why I'm sharing, they want to know, "What's the justification, what's the benefit that I get from this?"

If they could say, "Well, I'm getting something that I can't get anywhere else, only the Government has it," I think that's something that's powerful. That's something where there's an immediate reason of, "Oh, OK, well, you're giving me visibility that I have no other mechanism to get, please keep sharing with them, I would like this to continue."

Those, I think, are the primary ways we can improve it.

Mr. DONOVAN. Thank you.

Mr. MAYER. Congressman, I would echo the remarks around small and medium business. I think all of the issues that were raised there are, in fact, the case with our sector.

What I would say is, in the case of the network service providers, especially from a critical infrastructure perspective, there's absolutely no disincentive to share, in fact just the opposite. There's a tremendous incentive to share.

It's very common. First of all, we have formal venues where on a weekly basis the network service providers convene and talk about what's going on on the networks and what they're seeing. On a quarterly basis, the chief information security officers of the largest internet service providers meet to talk about what's happening in the environment globally and what they're doing to mitigate those risks.

Importantly, when events arise, you immediately see the sector rallying to respond to those events. So, for example, in October 2016 when the Dyn attack occurred, our members, through the Comms–ISAC, immediately convened and were ready to respond in any way that was requested. We coordinated that activity through the National Coordinating Center.

So the nature of the networks and their interdependencies and interconnection mitigates, I think, against any interest in not sharing information that impacts the network.

This has been going on for quite a while. It's quite sophisticated. It's often, you know, private and behind the scenes. It does involve Government when necessary.

So I think that it's a very effective mechanism, and we learn from our experiences with each event and it's gotten more refined.

Mr. DONOVAN. Great. I thank you. All my time has expired, Mr. Chairman.

Mr. RATCLIFFE. I thank the gentleman.

The Chair now recognizes the gentlelady from Texas, Ms. Jackson Lee, for 5 minutes.

Ms. JACKSON LEE. Thank you, Mr. Chairman, and to the Ranking Member.

I would like to, before I start, take a moment of personal privilege to acknowledge the Texas National Guard and their leadership development class program. So if they would stand.

We appreciate your presence here today.

I want to applaud them for all the work that they did during Hurricane Harvey. You have at least two Texans in the room, I believe, with the Chairman.

So we are greatly appreciative. As soon as I finish my questioning, I look forward to chatting with you. Thank you all very much.

Mr. RATCLIFFE. Thank you. I'm sure I can safely say that all Texans thank you for your efforts in those regards.

The gentlelady is recognized.

Ms. JACKSON LEE. I thank you. It looks like the clock has run, but I thank the Chairman for his indulgence.

Let me just read a statement that I thought was particularly potent and I think all of us can reflect over.

Over the past year Russian actors targeted U.S. election infrastructure. Of course, they are not my words, but words from the intelligence community and particularly the Office of Director of National Intelligence.

Hackers escalated efforts to breach the domestic energy sector and WannaCry and NotPetya ransomware wreaked havoc on public and private infrastructure around the world. According to Symantec, the world of cyber espionage experienced a notable shift toward more overt activity designed to destabilize and disrupt targeted organizations and countries.

Let me also acknowledge that the NPPD Office of Cybersecurity and Communications, specifically the National Cybersecurity and Communications Integration Center, carries out the bulk of our DHS responsibilities relating to facilitating the sharing of cyber threat information. It is a fixture that we have in place.

Although DHS is authorized to deploy a range of tools, resources, and programs to carry out its cyber mission, it has limited authority to regulate privately-owned networks and cannot require private entities to adopt specific security measures, grant access to their systems, or share information.

So I am applauding and I do think it is important that we have this hearing, but I would like to emphasize with the level of breach that we experienced that this requires as much a concern about the private sector as it requires patriotism and the recognition that we must find a common path that gives comfort to the layered tech industry but as well protects the American people.

I don't think any of you sitting here, of whom I appreciate very much your presence, want to be part of a breached electoral system, one that is not reliable, one that does not equate to the democratic principles that we are so attuned to.

So as I pose my questions, I'm hoping that we can find a pathway. I am very interested in the thoughts offered that suggested that we must make it easy. We should not have to stand up new technology which means we don't have to complicate it for you. Then, of course, "what's in it for us?". That's a little difficult for me on the "what's in it for us?" because I'm not sure I fully understand what would have to be in it for us.

So why don't I go to the witness who indicated that, and that would be Ms. Cagliostro.

What would it mean to say, "what is in it for us?"

Ms. CAGLIOSTRO. So when I say that, I mean in the context of you have to think about the return on investment for organizations. In cybersecurity it is an incredibly research—or, sorry, resource-strapped organization. CISOs are always asking for more

money. There are very few organizations, I'm sure, that have spending decreasing.

So when we think about information sharing, it is a cost like any other process or any other new tool or technique that we're going to bring on-line.

In order for that cost to make sense, we have to empower organizations with the answer for the ROI question. Is it that we're giving them visibility they don't have? Is it that we're helping them to protect organizations that are ultimately liabilities to them because they connect to their network?

So in the example of banks, big banks have connectivity into maybe smaller banks' networks. It is beneficial to share information with those smaller banks because they expose the bigger banks' network to risk.

So when I say the "what's in it for me?", I mean more in the context of ROI. I completely agree with you, I think that patriotism should play a role in this as well, but I think if we really want to see success there we have to help organizations answer the ROI question.

Ms. JACKSON LEE. So would it be that the exposure, publicity, I guess that part of—I mean, I don't think the Government can give monetary value. So what would be the kind of exposure that they wouldn't get that would be positive that we could be engaged in for them doing information sharing?

Ms. CAGLIOSTRO. I think that the Government has access to data, that is the thing that the Government has, and I believe the number was 2,200 indicators so far that have been declassified and released to industry.

I think that—so today there's something like 100 million indicators. It is in our platform alone. There's a tremendous amount of threat data that's available out there.

I think that the 2,200 number becomes a little bit less the large or an imposing number when you think about the context of available information. I think what Government can do is by accelerating and maybe increasing the level of what they're declassifying, then they're answering the question for industry and saying, "Hey, I'm now giving you data that you can't get anywhere else." There's value here because you can't go to a vendor and buy it. You can't go develop it internally.

Then that's an immediate quick answer that when a CISO or a CEO says, "Why am I sharing with the Government?" they say, because they're giving us visibility that we cannot achieve anywhere else and ultimately that's going to benefit our protections.

Ms. JACKSON LEE. Let me ask this question that if all of you would take a hit.

I have a third question, Mr. Chairman, and I'll be finished.

In your view, what do companies perceive is the value of sharing information with DHS—and you have answered it partly, but I would like to hear the other members—recognizing that there are issues with the timeliness and usefulness of some shared threat data? What features of DHS bulletins, alerts, and other products do companies find helpful? As well as what do you think is—so the value, and then what do you think the biggest challenge is?

I would like to start with the first witness because I was interested in your comments about what would be helpful is determining or we should be determining how the cyber incident happened and what can we do to protect ourselves.

I noticed that you said we can't require it, but I'm really looking for a way that we don't use the word "require," but we have a cohesive relationship that it is beneficial that I'm willing to act positively to do it and it will help both business and government. So somewhere short of requiring, but obviously it has to be mutual benefit, as has been said.

But the challenges and the value of sharing information.

Mr. KNAKE. Yes, ma'am.

I look at this—I look to the Department of Defense as a model on this. What the Defense Cyber Crime Center has done with their DIBnet program is they have created the mechanism by which companies can share, but they have also created a reason to share. It is really because they take a customer service approach to their community.

If you as a DIB company share information with DCCC, they will share information that is pertinent back to you and to the rest of the community.

You say, "We saw this activity on our network," they'll push that through the intelligence community. They'll come back to you and say, "Oh, that may be related to this, this, and this." They'll give you mitigation methods, they will do malware analysis, and they will push the findings from that analysis back to you.

So I think if you want to get more information coming into DHS you need to think not in terms of the volume of overall data that you get back by participating, but what do you get back specifically related to the information that you share in. That would be how you would create a higher volume of information coming into Government.

Ms. JACKSON LEE. So it would have to be relevant to the particular producer of information sharing?

Mr. KNAKE. Yes, ma'am.

Ms. JACKSON LEE. Would that be the gist of it?

Ms. Barron-Dicamillo.

Ms. BARRON-DICAMILLO. Yes, I agree with Rob and the challenge. I think I would say it is really to help operators institutionalize this information within their environments, they need to be able to almost share playbook-type details. So that kinds of context that, you know, that's going to be specific to how I would implement these indicators within my environment, which is more than just an IP address or a URL.

So the playbook-type details that you need to implement this is just not available in a lot of the current information-sharing systems. But the value is definitely inherent in all information-sharing programs, and it comes down to one person's detection is another person's prevention.

So between these two, the value and the challenge, collectively, the ability to bring those two things together, and technology and these information-sharing programs are coalescing on those two that we're seeing through the evolution of better capabilities, more available systems, and such.

Ms. JACKSON LEE. I don't know if you want to add anymore.

Ms. CAGLIOSTRO. Sure. So I want to agree with Ann on what she discussed with the context, because what tends to happen is that if organizations don't have that additional context, I think that's kind-of the easiest step to what I talked about with that return on investment. Even if it is not net new intelligence, but a course of action or a recommendation, I think that can be really helpful, as well.

Ms. JACKSON LEE. Mr. Mayer.

Mr. MAYER. Congresswoman, thank you.

I think you alluded to the fact that we're increasingly seeing nation-state attacks. That's just the reality of the environment right now.

Ms. JACKSON LEE. Yes.

Mr. MAYER. In light of that, the Government brings very unique capabilities, especially within the context of the intelligence community, to bring contextual light to what the campaign is, who are the targets, what's at risk.

Recently we have seen, and it is very encouraging, DHS invite more communications about providing context around some of these activities, advanced persistent threats, as they're called.

The challenge for us, and it is very frustrating as you can imagine, is that there are instances where Classified information might be shared with people who are cleared, but the actionable part requires sharing that information with people inside your organizations who might not be cleared. That frustration is real and we have to work to resolve that.

One of the ways we can do that, and DHS has offered to do this, is we need to create tear-lines, and we need to bring the technical people to the table so they can understand not necessarily the attribution, but what does the campaign look like, what's the context, who are the targets, what are we seeing. That's a two-way street.

So just like we said we can't legislate confidence, we can't legislate trust, but we can start building that trust, and I think we are beginning to see that evolve. The question is can we ramp it up quickly enough in light of the accelerating attacks that we're experiencing.

Ms. JACKSON LEE. Mr. Chairman, I had—this was a third question.

Mr. RATCLIFFE. Yes, I'm sorry. The gentlelady's time has expired. The gentleman from Virginia has a 4 o'clock appointment, and I want to give him an opportunity to ask questions.

Ms. JACKSON LEE. Can I just put my question on the record, and then I'll yield to this gentleman if I can?

Mr. RATCLIFFE. You can.

Ms. JACKSON LEE. It was to you, Mr. Mayer, because of—and I keep thinking of call you mayor, so I'm trying to find out what city you're the mayor of. Mayor of cyber threats.

But can you think about this? I will see whether or not I'm still here after the gentleman speaks. But you were concerned that we're learning a lot about—are we learning enough to react to the evolving cyber threats?

Then last, this whole issue of new devices. Are we learning enough about new devices? My position is that we need a lot of work in that area.

So thank you for allowing me put the question on the record.

Mr. RATCLIFFE. The gentlelady's time has expired.

The gentleman from Virginia, Mr. Garrett, is recognized.

Mr. GARRETT. So it is my pleasure. I thank the gentlelady from Texas for some really good questions that I think dovetail relatively well with what we have in our 5 minutes.

We talked about the actors being either nation-states or non-nation-states. I think that speaks to the nature of the threat. It troubles me because historically the paradigm of existential threats—and, obviously a lot of you all are involved in the private sector.

But I think that Mr. Knake nailed it when he talked about the tragedy of the commons. If there's not cross-communication we're lost. If we learn from the attacks on the grid in the Ukraine or sort-of the probes in the Baltic States we understand that what might be used against the public sector one day may be used against the private sector the next. It really doesn't matter who the threat is, but it is different than what we faced in the past.

So I wonder—and by the way, I want to get this on the record, Andy Greenberg's work, particularly in *Wired,* June 20, 2017, and his book, "How to Switch a Country Off," which I'm sure you all are familiar with, to the extent that there's stuff that's outside the realm of Classified that can be enlightening to individuals in the room and perhaps abroad who are interested in learning about this, that is sort-of sobering.

Having said all of that, I'm an advocate for limited government. Having said that, if we don't information share, we're lost. If we look, I think, at what happened in Ukraine, almost everything that was used to flip the lights on and off at will on a time line at the choosing of the attackers was off-the-shelf, but the white list-black list information wasn't shared, and so it wasn't caught.

Can you speak to the nature of how important it is to communicate privately, publicly, and with one another? I would love to get a 10- or 20-second bite on the nature of the threat, if you could give a 1 to 10 scale as it relates to the existential nature of the cyber threat. I think I know the answer. I want to hear from the experts and I want it on the record because I think America needs to know the answer.

We'll just work out way down the panel.

Mr. KNAKE. Thank you, Congressman.

I would say that the expectation we should have is that everything we've seen happening overseas will happen in the United States under the right geopolitical circumstances. If the lights have gotten turned off in Ukraine when Russians saw fit to turn the lights off in Ukraine, the lights will get turned off in the United States when Russians see that it's in their interest to do that.

So I think from that perspective we need to be planning, and we need to be planning not just for how we protect the grid but how we will respond and recover.

Mr. GARRETT. You're not a preparedness guy, but the impact of the lights going off is dead people, right? I mean, literally human lives are lost when the electricity goes out, whether it's people on

ventilators, whether it's people who need their medicines refrigerated, et cetera, right?

Again, I know the answer, you know the answer, but this needs to be out there so that the American people understand the gravity of the answer. But that's fair to say, right, human life would be the consequence?

Mr. KNAKE. Yes. I think the important thing is to make our adversaries aware that we will view that as the consequence and we will respond accordingly on a National level.

Mr. GARRETT. We can move down the table. I've got a finite amount of time.

Ms. BARRON-DICAMILLO. So I would say it is important to remember that a lot of the advanced persistent threat actors moonlight as cyber criminals. So they are using the same tools in their day job that they're using in the evening against—you know, for criminal or for monetary-type initiatives.

So you have to look at them as the collective and look at the tactics, techniques, and procedures in a collective in order to be effective.

Mr. GARRETT. I'm not even going to try to butcher your name, ma'am.

Ms. CAGLIOSTRO. It happens all the time.

So you mentioned existential threat. I think those are scary words, and I think they're appropriate words.

What's new—the threat is not new. We've always had conflict with other nations. There's always been pressure there. What's new is the reach that technology brings into our lives. The nation-state can—I have a cell phone, I have a watch. When you get into medical technology and device technology it is literally implanted in your body. Self-driving cars.

As you see this evolve the existential threat continues to grow because it just becomes a larger and more personal way that you can be touched and attacked.

Mr. GARRETT. The scale—Mr. Mayer, we're going to get to you—and the scale required to launch a decisive or debilitating attack against a nation-state, it used to be measured in cavalry or battle ships or battle tanks or fighter planes, and now it can be an actor with internet access, correct?

Ms. CAGLIOSTRO. Correct. Over the summer, I believe, or some point earlier this year, there was a botnet that used different devices, not traditional computers, servers, things like that. They infected devices that are in your homes. Because of the prevalence and the availability of those they were able to create a pretty powerful botnet that could deny service. So that's definitely something that——

Mr. GARRETT. Mr. Chair, I'm about to run out of time. I want to give Mr. Mayer a chance. But what I want to do here today is draw on the expertise of these folks, again sort-of recommend Andy Greenberg's work to the lay public, and certainly look forward to talking more about this moving forward.

Because another thing that's refreshing is the bipartisan nature, I think, of the fact that we are addressing this. Sure, people want to score political points. Yes, the Russians are bad actors. This is about America's existential future.

I think that the takeaway needs to be that the communication has to be public-private, and it has to be free-flowing, because if the Ukrainians had good communication a lot of these things perhaps are stopped because their systems are updated to recognize the malware that was used against them, at least theoretically.

But if it doesn't get updated every month—or every day even—off-the-shelf stuff brings the whole grid down.

Mr. Mayer, I'm sorry, and I'm done.

Mr. MAYER. No, thank you, Congressman. Real quickly, there's no question, I mean, the exponential growth of IoT devices presents a serious risk to networks in terms of how distributed denial-of-service attacks can occur, and there's a lot of work being done to implement defense mechanisms.

But I want to just refer to something on US–CERT. It is in the—it is a top item on the alert. It is Unclassified. It speaks to a campaign against critical infrastructure involving electricity, water, transportation, and some others. All of the information or a good part of the information is in TLP, traffic light protocol white, and there's whole series of activities that can be done.

That kind of information that's provided by the Government is invaluable and needs to get dispersed widely, not just in terms of remediating the problem, but making people aware of how significant the threat is, which is what I think you're speaking to.

Coming from the public to encourage greater Government and industry collaboration in this area is very important. I think that it is bipartisan. I think that every Member of Congress can help move that forward.

Mr. GARRETT. Thank you. I apologize for going over.

Mr. RATCLIFFE. No apology necessary.

I thank all of the witnesses for your testimony today. I thank all of the Members for their thoughtful questions.

Members of the committee may have, in fact are likely to have some additional questions for the witnesses, and we'll ask you to respond to those in writing.

Pursuant to Committee Rule VII(D), the hearing record will remain open for a period of 10 days.

Without objection, the subcommittee stands adjourned.

[Whereupon, at 4:04 p.m., the subcommittee was adjourned.]

APPENDIX

QUESTIONS FROM CONGRESSMAN JAMES R. LANGEVIN FOR ROBERT K. KNAKE

Question 1. In your position paper, you identified multiple obstacles in establishing a "FINnet", including the lack of cleared personnel, the absence of secure facilities, and a strong cultural difference regarding the handling of Classified material. Most significantly, the financial sector differs from the Defense Industrial Base in that it conducts business in the public domain as opposed to within the Classified spaces. How would Classified material shared on FINnet (or the CINet mentioned in the hearing) be utilized to defend Unclassified networks?

Answer. If CInet were developed, the utilization of Classified information by the financial services industry and other sectors would be substantially the same as within the Defense Industrial Base (DIB). Classified information shared by DOD over the DIBnet is shared for the purpose of helping DIB companies defend their Unclassified business networks from threat actors.

As with the DOD program, companies would not take Classified information off of Classified networks and use that information on Unclassified networks. To do so, would put at risk sources and methods used to collect the information as well as violate the law, which provides substantial penalties. Instead, indicators of compromise that relate to Classified threat information would either be downgraded so they can be used in Unclassified network defense activity or fed into the Enhanced Cybersecurity Services (ECS) program, which utilizes Classified indicators to detect and block attacks.

A network like CInet would provide two things: (1) The context around threats; and (2) the ability to coordinate. On context, CInet would allow the intelligence community to explain the importance of certain indicators and what they may mean if detected within an organization. For instance, if an indicator is triggered by traffic run through the ECS program, companies would be able to communicate with Government agencies to understand what the indicator was for. At present, without this capability, companies participating in ECS have no knowledge of what the program has detected.

On coordination, when an organization discovers an incident or when law enforcement or the intelligence community have reason to suspect a compromise within an organization, CInet would be an invaluable tool. It would allow organizations to securely exchange information with Government and with partner organizations. Such communication might include both advice on remediation as well as information coming out of the victim organization that others could use to see if they are compromised or prevent a future compromise.

At the tactical level, participating companies would need to apply for facility clearances. They would then need to construct a secure storage area at the secret level—a Vault. They would need to hire or appoint a Facility Security Officer who would be legally responsible for ensuring that Classified information is protected. Companies would likely choose to locate their Vault's close to their Security Operations Centers (SOCs). A Vault would likely include one or more terminals that would connect to the Classified network. Each terminal would consist of a laptop and phone. Many companies would likely choose to have a small conference table within the Vault for Classified discussions. Information obtained on the Classified network would be used to help guide decisions for protecting the Unclassified network. Crucially, only officials within the company who have the appropriate clearance and the requisite "need to know" would participate in these discussions.

The investment needed to stand up such an operation is relatively small for these organizations, many of whom have security budgets in the hundreds of millions of dollars; however, a good interim step might be to establish the network but place terminals in existing Government or defense contractor facilities. Organizations with cleared personnel could be stationed at these facilities or visit these facilities on an as-needed basis.

It is also important to note that the Financial Services industry has recruited heavily from the U.S. military, intelligence community, civilian agencies, and defense contractors. Of the eight Global Systemically Important Banks (G–SIBs)[1] that are based in the United States, five have Chief Information Security Officers (CISOs), or equivalent, with backgrounds in National security. For instance, the head of global cybersecurity at Citibank was previously the director of the National Cybersecurity & Communications Integration Center at DHS; the CISO at JP Morgan, came there from Lockheed Martin; the CISO at Goldman Sachs is the former assitant secretary of cybersecurity & communications at the Department of Homeland Security (DHS); the CISO at Wells Fargo is a retired Naval Officer who served at the NSA; and the CISO at Bank of New York Mellon spent 19 years at Booz Allen prior to taking on that role.

All these firms have hired team members below the CISO with Government or defense experience as have many other leading institutions. All have personnel that have maintained their clearances from Government or military service or received clearances from DHS. Many have built out intelligence fusion centers that rival the capabilities of Government agencies. They are actively tracking actor sets as these actors target their systems and are continuously sharing information with each other. In my view, they are at a stage of maturity where real-time sharing of Classified information would be useful and warranted.

Question 2a. What would give companies an incentive to participate in a cyber NTSB given the evident reputational risks involved?

Answer. For a Cyber NTSB to succeed, it will be crucial that companies are obligated to participate before an incident occurs. While an incident is unfolding, companies will always believe that the risks of sharing information about the incident outweigh the benefits. The reason for that is simple: No benefits will accrue directly to them. The value in sharing this information goes to the security of other companies that are receiving the information and, in no small part, to the National security of the United States. If, on the other hand, companies receive a benefit, such as Federally-backstopped cyber insurance, for commiting to notifying the Cyber NTSB and having its team come in in the event of an incident, the risks could be managed.

Question 2b. Can Congress reduce these risks?

Answer. Congress could reduce these risks by establishing the program in coordination with industry and directing relevant Federal agencies to develop rules that would ensure the anonymity of participating companies. Cogress should also ensure that information shared under the program is protected from regulatory agencies as under the existing Protected Critical Infrastructure Information program. Of course, such protections should not exempt companies from meeting any obligations to disclose incidents to regulators.

Question 2c. How can no-fault post mortems be encouraged across the cybersecurity landscape?

Answer. I continue to believe that the best way to promote no-fault post mortems is with insurance. A binding requirement through insurance contracts, whether backed by the Federal Government or by the insurance industry without Federal support, would provide the legal basis necessary to gain commitments to engaging in post-mortem information-sharing programs.

QUESTIONS FROM HONORABLE JAMES R. LANGEVIN FOR ANN BARRON-DICAMILLO

Question 1a. Can you describe your involvement with both the DHS Cyber Information Sharing and Collaboration Program (CISCP) and the Automated Indicator Sharing (AIS) program?

Question 1b. What are your engagements with the leadership of each?

Question 1c. Have you run into any obstacles to your active participation in each?

Question 1d. What is your plan for being an active participant in each?

Answer. We currently receive the CISCP data via FS–ISAC and have no plans to change that process. We were informed by DHS that participating directly in the CISCP program would preclude the ability of additional AXP employees obtaining security clearances through the Private-Sector Clearance Program due to DoD policy.

We do not currently participate in the AIS program but have been evaluating that program for possible future participation. We met recently with DHS leadership about both the CISCP and AIS programs. Our understanding from these discussions is that the data from the two programs has substantial overlap. We also have con-

[1] *http://www.fsb.org/wp-content/uploads/2016-list-of-global-systemically-important-banks-G-SIBs.pdf.*

cerns about the validation of the data and the vetting of the participants for AIS. One of our current threat intelligence vendors is in the process of consuming AIS data which will then be validated. Once we have verified that process, we will further evaluate AIS participation.

Question 2a. The Cybersecurity Act of 2015 made substantial changes to the legal authorities regarding cyber threat indicator sharing. What specific activities is your organization carrying out today thanks to those authorities and liability protections?

Question 2b. What is your assessment of the effectiveness of the current liability protections?

Answer. We have formalized our internal standards and operational procedures with regard to cyber threat indicator sharing to comply with the law. Our teams carry out these processes on a daily basis so we take advantage of these authorities and protections constantly. While the liability protections have not been tested in practice, we do believe that such protections encourage the sharing of threat indicators.

Question 3. Have you utilized the previously Classified indicators that are provided within the AIS data feed to improve the protection of your networks?

Our understanding is that we already obtain previously Classified indicators shared by Government participants of AIS via the CISCP reports to FS–ISAC.

Question 4. What changes to AIS and supporting activities do you recommend to improve the effectiveness of the program?

Answer. We recommend the following enhancements to AIS to improve the effectiveness of the program:

- Add support for STIX 2.0.
- Alleviate trust concerns for outbound sharing by additional vetting of participants or supporting multiple trust levels or communities of interest for sharing beyond the existing options of DHS only, all USG, or all AIS participants.
- Address data quality concerns through development of best practices, training, and mechanisms for assessing and providing feedback to participants.

Question 5. In your written testimony, you mention quality versus quantity of threat indicator information.

Is there a need for high throughput data shared at "machine speed" even if it hasn't been thoroughly analyzed yet?

Question 5b. Can companies conduct meaningful analysis on indicators shared through AIS absent contextual information, or is that essential for the indicators to be useful? What basis do you have for making that determination?

Question 5c. Are the privacy protections put in place under the Cybersecurity Act of 2015 adequate, particularly if indicators need to be analyzed before sharing, which would allow time for more thorough privacy reviews?

Answer. High-speed data is not very valuable without context. High throughput can lead to more "noise" in the system and can be paralyzing for less sophisticated organizations to act upon.

Companies can potentially conduct meaningful analysis of AIS data without context but this requires more resources to validate and curate that data. The cybersecurity industry has coalesced around the need for more contextual information sharing as evidenced by Cyber Threat Intelligence vendors producing information-sharing playbooks.

The challenge of privacy protections is that what constitutes personal information is shifting and changing with new technologies, and what information is sufficient to identify a specific individual also changes with context and technology. The DHS "Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015" is a helpful document which identifies some categories of personal information which is unlikely to be directly related to a cybersecurity threat, but we suspect this guidance should be periodically updated.

We do think that the privacy protections, between the guidance to non-Federal entities and the further guidance to Federal entities and DHS on required reviews of specific fields such as raw email message bodies, appear to be sufficient to protect personal privacy and have not been a major impediment to participation in these programs.

QUESTION FROM HONORABLE JAMES R. LANGEVIN FOR PATRICIA CAGLIOSTRO

Question. What changes to AIS and supporting activities do you recommend to improve the effectiveness of the program?

Answer.

1. Incentivize organizations to share back to AIS by enriching the intelligence with additional data and require organizations to share to gain access. The Gov-

ernment has unmatched visibility and intelligence available in Unclassified and Classified environments. This data can be used to enrich shared intelligence that organizations do not have access to. By using this data to enrich the intelligence and limiting only to organizations that share intelligence back to AIS, you create an incentive to encourage organizations to share rather than just consume. For example, an organization shares an IP address and the Government knows that IP address is associated with a campaign that affects the financial services industry. The Government would enrich the shared indicator with this information and share the enriched indicator with organizations that share with AIS.

2. Create a grant program for security companies to develop bi-directional integrations with AIS. Today, many organizations consume and integrate AIS with their security tools, but there is limited availability of bi-directional integrations. Analysts collect and produce cyber threat intelligence as part of their daily workflow. In the Anomali platform, analysts simply check a box to automatically share intelligence with their community. They are more likely to share because it's integrated with their daily workflows, rather than an additional step or technology they must work with. AIS will benefit greatly from bi-directional integration with the tools that they perform their daily work in. This requires development resources from the security industry. The Government could create a grant program for the security industry to pay for the development required to create bi-directional integrations with the AIS program.

QUESTIONS FROM HONORABLE JAMES R. LANGEVIN FOR ROBERT H. MAYER

Question 1a. The Cybersecurity Act of 2015 made substantial changes to the legal authorities regarding cyber threat indicator sharing. What specific activities are your member organizations carrying out today thanks to those authorities and liability protections?

Answer. The ability to share information about cyber threats and effective countermeasures among industry players and between industry and Government is crucial, and the explicit liability protections for sharing in accordance with Cybersecurity Information Sharing Act (CISA) were welcome, as were the authorizations to monitor information systems and share or receive cyber threat indicators and defensive measures. The communications sector participates in structured cybersecurity information sharing through, for example, the Communications Information Sharing and Analysis Center (Comm–ISAC), the National Cybersecurity and Communications Integration Center (NCCIC), DHS's Communications Sector Coordination Council (CSCC), the National Security Telecommunications Advisory Committee (NSTAC), United States Computer Emergency Readiness Team (US–CERT), CTIA's Cybersecurity Working Group (CSWG), and among others.

Since the passage of the CISA in 2015, we have focused on moving beyond information-sharing trials to automated sharing via new technologies. CTIA, through its Cyber Threat Information Sharing Pilot, has been working with large, medium, and small companies in both the wireless and wireline segments to support industry efforts to share cyber threat indicators and facilitate integration with the DHS Automated Information Sharing portal. The pilot program was completed this year and made strides to test the ability to automate the sharing of threat information among carriers to rapidly and effectively mitigate cyber threats, specifically focusing on Telephony Denial-of-Service (TDoS) attacks.

Question 1b. What is your assessment of the effectiveness of the current liability protections?

Answer. While CISA has provided greater confidence to the private sector in their ability to share cyber threat indicators by removing certain legal barriers, valid concerns about liability remain. As an example, last year the Automotive Information Sharing and Analysis Center (Auto–ISAC) was subpoenaed as part of an on-going class-action lawsuit against Fiat Chrysler. While the Auto–ISAC was able to successfully quash the subpoena, the ordeal has reportedly had a chilling effect on participant's willingness to share information.[1] There was another example of a broker and a security researcher teaming up to publicly release a vulnerability in a medical device in an apparent effort to short the stock of a medical device manufacturer.[2] As a result of examples like these, companies must still conduct thorough legal and risk analyses before sharing cyber threat information. These reviews, while nec-

[1] Joshua Higgins, Head of auto industry's ISAC cites "chilling effect" of lawsuit on cyber info-sharing, Inside Cybersecurity (Nov. 2, 2017).

[2] See Linette Lopez, Carson Block has a new short, and his reasoning is super creepy, Business Insider (Aug. 25, 2016).

essary, can potentially result in delayed sharing or an unwillingness to share until uncertainties surrounding liability are resolved.

Question 2. Have your member organizations utilized the previously Classified indicators that are provided within the AIS data feed?

Answer. Yes, our members conducted an automated cyber-threat information-sharing pilot, that concluded in 2017, and the AIS data feed was incorporated into the effort. Other members receive AIS feeds on a regular basis and review and pass along information to front-line resources when it is timely, appropriately contextualized and therefore actionable.

Question 3. What changes to AIS and supporting activities do you recommend to improve the effectiveness of the program?

Answer. Based on the pilot experience referenced in response to question 2 above, the pilot participants explored use cases and scenarios associated with telecom-specific threats that are not currently covered in the AIS vocabulary.

In particular, the pilot addressed Robocall trace-back and Telephony Denial-of-Service (TDoS) threat scenarios as well as SS7 Blacklist Global Title information sharing.

Given that AIS focuses on the sharing of declassified indicators shared at the un-Classified level, we would support the continued efforts of the participating AIS Federal agencies to declassify indicators and to enrich the contextual information provided with the indicators.