FEBRUARY 25, 2015

EXAMINING THE PRESIDENT'S CYBERSECURITY INFORMATION SHARING PROPOSAL

U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON HOMELAND SECURITY

ONE HUNDRED FOURTEENTH CONGRESS, FIRST SESSION

HEARING CONTENTS:

MEMBER STATEMENTS:

WITNESSES:

AVAILABLE WEBCAST(S):*

Chairman's Opening Statement: *https://www.youtube.com/watch?v=NuhLtlC14IE*

Witness Questioning: *https://www.youtube.com/watch?v=TEZBOxtSnrI*

COMPILED FROM:

https://homeland.house.gov/hearing/hearing-administration-s-cybersecurity-legislative-proposal-information-sharing

** Please note: Any external links included in this compilation were functional at its creation but are not maintained thereafter.*

Committee on
HOMELAND SECURITY
Chairman Michael McCaul

Opening Statement

February 25, 2015

Media Contact: April Ward
(202) 226-8477

Statement of Chairman Michael McCaul (R-Texas)
Committee on Homeland Security

"Examining the President's Cybersecurity Information Sharing Proposal"

Remarks as Delivered

At the dawn of the digital age, our nation saw endless opportunities to generate prosperity by expanding our networks and connecting to the world. But today, American prosperity depends as much on defending those networks as it does on expanding them.

Every day our country faces digital intrusions from criminals, hacktivists, terrorists, and nation-states like Russia, China and Iran. The impacts of those intrusions are felt everywhere—from our national security secrets to the personal information of Americans.

We cannot tolerate acts of cyber vandalism, cyber theft, and cyber warfare especially when they put our nation's critical infrastructure at risk and when they steal American intellectual property and innovation. Accordingly, our government must play a leading role in combating threats in the digital domain.

It is clear that safeguarding American cyberspace is one of the great national security challenges of our time. We are confronted almost daily with frightening new precedents, such as the North Korean cyber attack on Sony Pictures—a cowardly act meant to intimidate Americans and stifle freedom of expression.

This attack came from a nation-state using a digital bomb to target and destroy computer systems here in the United States. Iranian-backed hackers also demonstrated this capability when they attacked Saudi Arabia's national oil company, Aramco, and destroyed 30,000 computers. Iran also continues to target major U.S. banks to shut down websites and restrict Americans ability to access their bank accounts.

Imagine this type of attack on our gas pipelines or power grid in the Northeast. Such assaults on our critical infrastructure could cripple our economy and weaken our ability to defend the United States. These scenarios sometimes sound alarmist, but we must take them seriously as they grow more realistic

every day. Our adversaries are hard at work developing and refining cyber attack capabilities, and they are using them to intimidate our government and threaten our people in both times of peace and times of conflict.

But the threat extends beyond the industrial engines that drive our economy to the homes of Americans themselves. Criminals and countries alike can use cyber attacks to raid Americans' savings accounts or steal their personal health records.

The recent breach of health insurer, Anthem, illustrates the intrusiveness of these attacks. That assault alone exposed the personal information of up to 80 million people, including the names, birth dates, and social security numbers of tens of millions of children. But this is just the latest in a long string of cyber breaches targeting private citizens—a list that includes breaches at Target, Neiman Marcus, Home Depot, and JP Morgan.

Our adversaries are also seeking to steal secrets from our government and our most innovative companies. We know that Chinese hackers, for instance, continue to breach federal networks for the purpose of espionage and attack major U.S. businesses to give themselves a competitive edge in the global economy. Make no mistake: these attacks are costing Americans their time, money, and jobs. General Keith Alexander has described cyber espionage and the loss of American intellectual property as the "greatest transfer of wealth in history."

Sadly, our laws are not keeping up with the threat. For instance, fearing legal liability, many private companies choose to not disclose the threats they see on their own networks, leaving others vulnerable to the same intrusions.

We cannot leave the American people and our businesses to fend for themselves. Now, more than ever, Congress must take aggressive action.

This year I will lead a renewed effort to push cybersecurity legislation through Congress. Last year, the ranking member and I, and this committee, passed five cyber bills. These new statutes lay out the rules of the road on how cyber information will be shared between government and the private sector so that the two can work together to combat this persistent threat. The laws also provide important protections to ensure Americans' information and civil liberties are not compromised.

But now, we must build on that success. And, we can start by creating a "safe harbor" where legal barriers to sharing cyber threat information are removed and the private sector is encouraged to collaborate. This will allow us to respond to cyber incidents more quickly and effectively—and will give government and private entities the ability to see the threat landscape in real-time.

I am pleased the president has come forward with a proposal on this important issue. Our solutions must transcend partisan boundaries if we are going to tackle this challenge. The American people are counting on us.

I want to thank the witnesses for testifying before this committee and I look forward to your testimony.

###

Statement for the Record

The Honorable Suzanne E. Spaulding
Under Secretary, National Protection and Programs Directorate

Dr. Phyllis Schneck
Deputy Under Secretary, Cybersecurity and Communications

U.S. Department of Homeland Security

Before the
United States House of Representatives
Committee on Homeland Security

Regarding

Examining the President's Cybersecurity Information Sharing Proposal

February 25, 2015

Introduction

Chairman McCaul, Ranking Member Thompson, and distinguished Members of the Committee, we are pleased to appear today to discuss the President's cybersecurity legislative proposal on information sharing.

In our testimony today, we will highlight the Department of Homeland Security (DHS) National Protection and Programs Directorate cybersecurity role and capabilities, and describe how the President's legislative proposal to facilitate cyber threat indicator information sharing will further our national security, with DHS's National Cybersecurity and Communications Integration Center (NCCIC) as the coordination center to receive and disclose cyber threat indicators to Federal and Non-Federal entities.

The Ongoing Cyber Threat and the DHS Cybersecurity Role

As a nation, we are faced with pervasive cyber threats. Malicious actors, including those at nation-state level, are motivated by a variety of reasons that include espionage, political and ideological beliefs, and financial gain. Increasingly, State, Local, Tribal and Territorial (SLTT) networks are experiencing cyber activity of a sophistication level similar to that seen on Federal networks.

To achieve our cybersecurity mission, the National Protection and Programs Directorate focuses on helping our partners understand and manage cyber risk, reduce the frequency and impact of cyber incidents, and build partner capacity. We share timely and accurate information and analysis to enable private and public sector partners to protect themselves. We provide on-site assistance to Federal agencies and critical infrastructure entities impacted by a significant cybersecurity incident. We provide technology and services to detect and block cyber threats from impacting Federal civilian networks. We enable Federal agencies to more readily identify network security issues and take prioritized action. We enable commercial cybersecurity companies to use classified information so they can better protect their private sector customers. We perform comprehensive consequence analyses that assess cross-sector interdependencies and cascading effects, including the potential for kinetic harm that includes loss of life, and we maintain a trusted environment for private sector partners to share information and collaborate on cybersecurity threats and trends.

DHS's National Cybersecurity and Communications Integration Center

The NCCIC serves as a 24x7 centralized location for the coordination and integration of cyber situational awareness and incident management. NCCIC partners include all Federal departments and agencies; state, local, tribal, and territorial governments; the private sector; and international entities. The NCCIC continues to explore opportunities to expand its liaison capacity from other agencies and the private sector. The NCCIC provides its partners with enhanced situational awareness of cybersecurity and communications incidents and risks, and provides timely information to manage vulnerabilities, threats, and incidents. In 2014, the NCCIC received over 97,000 incident reports, and issued nearly 12,000 actionable cyber-alerts or warnings. NCCIC teams also detected over 64,000 significant vulnerabilities on federal and non-federal systems and directly responded to 115 significant cyber incidents.

The NCCIC actively shares cyber threat indicators to and from multiple sources including private sector partners, the Intelligence Community, Federal Departments and Agencies, law enforcement, State, Local, Tribal and Territorial governments, and international governments. This sharing, which has been taking place for many years, takes many forms including person-to-person interactions on the NCCIC floor, manual exchange of information via e-mail and secure web portals, and more recently via automated, machine-to-machine exchanges in STIX and TAXII protocols. While all of these sharing methods have value, the cybersecurity community has recognized the strategic importance of migrating cyber threat indicator sharing to more automated mechanisms when and where appropriate.

Cybersecurity Legislation

Last year, Congress acted in a bipartisan manner to pass critical cybersecurity legislation that enhanced the ability of the Department of Homeland Security to work with the private sector and other Federal civilian departments in each of their own cybersecurity activities, and enhanced the Department's cyber workforce authorities. Enactment of these bills represents a significant moment for the Department's cybersecurity mission, and this Committee in particular undertook significant efforts to bring the bills to passage. We are thankful for your support and we are deploying those additional authorities with clarity of mission.

Additional legislation is needed. We must take additional steps to ensure that DHS is able to rapidly and efficiently deploy new protective technologies across Federal civilian agency information systems. In addition, carefully updating laws to facilitate cybersecurity information sharing within the private sector and between the private and government sectors is also essential to improving the Nation's cybersecurity. While many companies currently share cybersecurity threat information under existing laws, there is a heightening need to increase the volume and speed of information shared without sacrificing the trust of the American people or the protection of privacy, confidentiality, civil rights, or civil liberties. It is essential to ensure that cyber threat information can be shared quickly among trusted partners, including with law enforcement, so that network owners and operators can take necessary steps to block threats and avoid damage.

The NCCIC plays a critical role in the President's recent legislative proposal because its core mission – as articulated in the National Cybersecurity Protection Act, developed by this Committee and unanimously-passed by the House in December – is to coordinate and serve as an interface for cybersecurity information across the government and private sector.

The Administration's Information Sharing Proposal for Cyber Threat Indicators

Building on the bipartisan cybersecurity legislation enacted last Congress, President Obama visited the NCCIC on January 13, 2015, to announce a proposal for additional legislation to improve cybersecurity information sharing. The President noted, "Much of our critical infrastructure runs on networks connected to the Internet….[a]nd most of this infrastructure is owned and operated by the private sector. So neither government nor the private sector can defend the nation alone. It's going to have to be a shared mission – government and industry working hand in hand, as partners." This partnership entails sharing cyber threat indicators to better enable government agencies and the private sector to protect themselves.

Information sharing, especially of these technical "threat indicators" that can be used to identify and block malicious activity, is the lifeblood of effective cyber defense and response. Pulling together this information allows defenders to identify anomalies or patterns and recognize dangerous activity before it can do significant damage. The goal of the President's proposal is to increase the sharing of this type of information, as quickly as possible, with appropriate protection for privacy and of sensitive information and systems.

Among other things, the Administration's proposal would reduce the risks for private entities to voluntarily share technical cyber threat indicators with each other and the NCCIC by providing protections against civil or criminal liability for such sharing. Equally important, the proposal narrowly defines the threat indicators that will be shared, requires that irrelevant identifying information be minimized from these indicators, and generally requires strong protections for the privacy and confidentiality of personal information. Finally, the proposal calls for the creation of Information Sharing and Analysis Organizations (ISAOs). ISAOs would be information sharing organizations that would help speed information sharing within the private sector and between the private sector and government.

Our goal is to expand information sharing within the private sector, and to build on the existing relationships, processes and programs of the NCCIC to enhance cooperation between the government and private sector. The proposal will help us improve the methods that the NCCIC already uses to share cyber threat indicators, and leverage automation to achieve scalability wherever possible. We look to evolve and expand indicator sharing at the NCCIC from human exchanges, portals, and written reports to automated machine-to-machine communications. Our vision is that this may reduce the time to receive and act on indicators from hours to milliseconds, create consistency in information provided to interagency partners, law enforcement, and the private sector, and free analysts to focus on the threats that require human analysis while expediting detection and blocking of new threats.

NCCIC as the Coordination Center

Cyber threat indicators, which allow government agencies and the private sector to better protect themselves, come from a variety of sources, including: government agencies, private companies, international partners, and ISAOs. Given the variety of formats used – and information that is included – when sharing such information, the government must have a central clearinghouse to ensure that privacy and confidentiality protections are consistently applied and that the right information reaches the right government and private sector entities.

DHS is a leader within the government when it comes to the development and operational implementation of privacy, confidentiality, and civil liberties policies. DHS was the first agency to have statutorily established Officers for Privacy and for Civil Rights and Civil Liberties. From its creation, DHS has built both privacy and civil liberties protections into all of its programs and has dedicated, on-site privacy professionals committed to ensuring that its cyber mission is carried out in a way consistent with our Nation's values. Through statutory protections like Protected Critical Infrastructure Information (PCII), DHS will continue to anonymize the identity of submitters and other proprietary and sensitive information in threat indicator submissions. Moreover, the President's proposal calls for DHS to build upon its existing privacy, confidentiality, and civil liberty procedures by working with the

Attorney General to develop new procedures to appropriately limit Government receipt, use, and retention of threat indicators. Establishing the NCCIC as the primary entry way for cyber threat indicators from the private sector will ensure uniform application of these important privacy and confidentiality protections, while still allowing cyber threat indictors to be shared with law enforcement for the specific purposes identified in the legislation.

NCCIC sits at the intersection of cyber communities, with representatives from the private sector and other government entities physically present on the NCCIC floor and connected virtually. This diverse participation in the NCCIC was cemented by section 226(d) of the Homeland Security Act as added by the National Cybersecurity Protection Act. NCCIC's core mission is to enable better network defense by assessing and appropriately sharing information on the risks to America's critical cyber systems and how to reduce them.

Building Capacity to Accelerate Automated Sharing of Cyber Threat Indicators

The Administration's proposal directs DHS to automate and share information in as close to real-time as practicable with relevant federal agencies, including law enforcement entities, and with ISAOs. For the past three years, DHS has led the development in collaboration with the private sector of specifications – known as STIX and TAXII – which standardize the representation and exchange of cyber threat information, including actionable cyber threat indicators. STIX, the Structured Threat Information eXpression, is a standardized format for the representation and exchange of cyber threat information, including indicators. TAXII, the Trusted Automated eXchange of Indicator Information, is a standardized protocol for discovering and exchanging cyber threat information in STIX. The interagency Enhance Shared Situational Awareness initiative has already chosen STIX as the basis for sharing cyber threat indicators between the Federal cyber centers, ensuring interoperability between these key sources of information.

Through collaboration between DHS and the private sector, there is a solid and rapidly growing base of commercial offerings supporting STIX and sharing indicators via the TAXII, including platforms, network protection appliances and endpoint security tools. While the NCCIC has in-house systems and tools to assist analysts in generating STIX indicators, those indicators are currently analyzed and filtered by human analysts and shared back out with the private sector and Federal partners through manual methods such as e-mail and secure portals. In 2014, the NCCIC began a limited pilot with several organizations to test automated delivery of STIX indicators via TAXII.

To inform our plan for achieving automated cyber threat indicator information sharing, DHS created a working group between a range of DHS offices and the FBI, a critical stakeholder in the NCCIC. We also included experts from our Privacy, Civil Rights and Civil Liberties, and Science and Technology offices, among others, to ensure that our architecture is based on best-in-class technology and is consistent with our values and our respect for Americans' privacy and civil liberties.

Implementation will proceed through four major phases: (1) an initial operating capability phase in which we will deploy a TAXII system that can disseminate STIX cyber threat indicators with increased automation capability, enabling the use of human analysis for the most complex problems and egregious threats; (2) an expanded automation phase in which we will develop and deploy DHS infrastructure that can receive, filter, and analyze cyber threat indicators-- during this phase, we will

promulgate guidance for private sector companies to minimize, redact and tag their data prior to submission to NCCIC, and will complete a Privacy Impact Assessment; (3) a final operating capability phase in which we will fully automate DHS processes to receive and appropriately disseminate cyber threat indicators in a machine-readable format and finalize policies for filtering, receipt, retention, use, and sharing, including regular compliance reviews; and (4) a scaled services capability phase, during which DHS will work to enable agencies that lack sufficient cybersecurity resources or expertise to receive and share cyber threat indicators with the NCCIC in near-real-time by providing a turnkey technical solution to "plug in" to the NCCIC.

DHS Shares Information Widely with Federal Agencies and the Private Sector

Currently, DHS shares information with Federal Agencies and the private sector. DHS takes a customer-focused approach to information sharing, and different types of information require differing response times and dissemination protocols. DHS provides information to detect and block cybersecurity attacks on Federal civilian agencies and shares information to help critical infrastructure entities in their own protection; provides information to commercial cybersecurity companies so they can better protect their customers through the Enhanced Cybersecurity Services program, or ECS; and maintains a trusted information sharing environment for private sector partners to share information and collaborate on cybersecurity threats and trends via a program known as the Cyber Information Sharing and Collaboration Program, or CISCP. This trust derives in large part from our emphasis on privacy, confidentiality, civil rights, and civil liberties across all information sharing programs, including special care to safeguard personally identifiable information.

DHS also directly supports Federal civilian departments and agencies in developing capabilities that will improve their own cybersecurity posture. Through the Continuous Diagnostics and Mitigation (CDM) program, DHS enables Federal agencies to more readily identify network security issues, including unauthorized and unmanaged hardware and software; known vulnerabilities; weak configuration settings; and potential insider attacks. Agencies can then prioritize mitigation of these issues based upon potential consequences or likelihood of exploitation by adversaries. The CDM program provides diagnostic sensors, tools, and dashboards that provide situational awareness to individual agencies, and will provide DHS with summary data to understand relative and system risk across the Executive Branch. DHS is moving aggressively to implement CDM across all Federal civilian agencies, and Memoranda of Agreement with the CDM program encompass over 97 percent of all Federal civilian personnel.

While CDM will identify vulnerabilities and systemic risks within agency networks, the National Cybersecurity Protection System, also known as EINSTEIN, detects and blocks threats at the perimeter of those networks or at an agencies' Internet Service Provider. EINSTEIN is an integrated intrusion detection, analysis, information sharing, and intrusion-prevention system. The most recent iteration, Einstein 3 Accelerated (E3a), supplements EINSTEIN 2 by adding additional intrusion prevention capabilities and enabling Internet Service Providers (ISPs), under the direction of DHS, to detect and block known or suspected cyber threats using indicators.

Conclusion

We are working together to find new and better ways to share accurate, timely data in a manner

consistent with fundamental American values of privacy, confidentiality, and civil rights. While securing cyberspace has been identified as a core DHS mission since the 2010 Quadrennial Homeland Security Review, the Department's view of cybersecurity has evolved to include a more holistic emphasis on critical infrastructure which takes into account the convergence of cyber and physical risk.

Today our adversaries exploit a fundamental asymmetry in our network infrastructure: while nearly all of our systems and networks are globally interconnected, our defensive capabilities are not. This gives the attackers a compelling advantage as they can find and exploit the weak links in our systems from anywhere around the world – at machine speed. By sharing cyber threat indicators in near real-time, we reduce that asymmetry.

As our defensive cybersecurity capabilities become more interconnected, we greatly reduce the likelihood that an adversary can re-use attack infrastructure, tools, tactics, techniques and procedures. In addition, we greatly reduce the time window in which new and novel attacks are effective because the ecosystem shares those indicators and develops a type of "herd immunity," improving defenses as indicators are shared and events are correlated in near-real-time. These two factors do not eliminate all cyber threats, but they hold the promise of significantly increasing the time and resources (both technical and human) that attackers must expend to achieve their goals. Moreover, the STIX data format and the TAXII transport method are increasingly compatible with commonly used commercial information technology (IT) products. This means more entities are able to send indicators automatically to the NCCIC, creating an ecosystem of indicators which will in turn provide greater context to malicious cyber activity and rapidly increase situational awareness per Executive Order 13636, *Improving Critical Infrastructure Cybersecurity* and Executive Order 13691, signed February 13, 2015, *Promoting Private Sector Cybersecurity Information Sharing*.

DHS will continue to serve as one of the government's primary resources for information sharing and collaborative analysis, at machine-speed wherever possible, of global cyber risks, trends, and incidents. Through our leadership role in protecting civilian government systems and helping the private sector protect itself, DHS can correlate data from diverse sources, in an anonymized and secure manner, to maximize insights and inform effective risk mitigation.

DHS provides the foundation of the U.S. government's approach to securing and ensuring the resilience of civilian critical infrastructure and essential services. We look forward to continuing the conversation and supporting the American goals of peace and stability; in these endeavors, we rely upon your continued support.

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

Statement for the Record

The Honorable Suzanne E. Spaulding
Under Secretary, National Protection and Programs Directorate

Dr. Phyllis Schneck
Deputy Under Secretary, Cybersecurity and Communications

U.S. Department of Homeland Security

Before the
United States House of Representatives
Committee on Homeland Security

Regarding

Examining the President's Cybersecurity Information Sharing Proposal

February 25, 2015

Introduction

Chairman McCaul, Ranking Member Thompson, and distinguished Members of the Committee, we are pleased to appear today to discuss the President's cybersecurity legislative proposal on information sharing.

In our testimony today, we will highlight the Department of Homeland Security (DHS) National Protection and Programs Directorate cybersecurity role and capabilities, and describe how the President's legislative proposal to facilitate cyber threat indicator information sharing will further our national security, with DHS's National Cybersecurity and Communications Integration Center (NCCIC) as the coordination center to receive and disclose cyber threat indicators to Federal and Non-Federal entities.

The Ongoing Cyber Threat and the DHS Cybersecurity Role

As a nation, we are faced with pervasive cyber threats. Malicious actors, including those at nation-state level, are motivated by a variety of reasons that include espionage, political and ideological beliefs, and financial gain. Increasingly, State, Local, Tribal and Territorial (SLTT) networks are experiencing cyber activity of a sophistication level similar to that seen on Federal networks.

To achieve our cybersecurity mission, the National Protection and Programs Directorate focuses on helping our partners understand and manage cyber risk, reduce the frequency and impact of cyber incidents, and build partner capacity. We share timely and accurate information and analysis to enable private and public sector partners to protect themselves. We provide on-site assistance to Federal agencies and critical infrastructure entities impacted by a significant cybersecurity incident. We provide technology and services to detect and block cyber threats from impacting Federal civilian networks. We enable Federal agencies to more readily identify network security issues and take prioritized action. We enable commercial cybersecurity companies to use classified information so they can better protect their private sector customers. We perform comprehensive consequence analyses that assess cross-sector interdependencies and cascading effects, including the potential for kinetic harm that includes loss of life, and we maintain a trusted environment for private sector partners to share information and collaborate on cybersecurity threats and trends.

DHS's National Cybersecurity and Communications Integration Center

The NCCIC serves as a 24x7 centralized location for the coordination and integration of cyber situational awareness and incident management. NCCIC partners include all Federal departments and agencies; state, local, tribal, and territorial governments; the private sector; and international entities. The NCCIC continues to explore opportunities to expand its liaison capacity from other agencies and the private sector. The NCCIC provides its partners with enhanced situational awareness of cybersecurity and communications incidents and risks, and provides timely information to manage vulnerabilities, threats, and incidents. In 2014, the NCCIC received over 97,000 incident reports, and issued nearly 12,000 actionable cyber-alerts or warnings. NCCIC teams also detected over 64,000 significant vulnerabilities on federal and non-federal systems and directly responded to 115 significant cyber incidents.

The NCCIC actively shares cyber threat indicators to and from multiple sources including private sector partners, the Intelligence Community, Federal Departments and Agencies, law enforcement, State, Local, Tribal and Territorial governments, and international governments. This sharing, which has been taking place for many years, takes many forms including person-to-person interactions on the NCCIC floor, manual exchange of information via e-mail and secure web portals, and more recently via automated, machine-to-machine exchanges in STIX and TAXII protocols. While all of these sharing methods have value, the cybersecurity community has recognized the strategic importance of migrating cyber threat indicator sharing to more automated mechanisms when and where appropriate.

Cybersecurity Legislation

Last year, Congress acted in a bipartisan manner to pass critical cybersecurity legislation that enhanced the ability of the Department of Homeland Security to work with the private sector and other Federal civilian departments in each of their own cybersecurity activities, and enhanced the Department's cyber workforce authorities. Enactment of these bills represents a significant moment for the Department's cybersecurity mission, and this Committee in particular undertook significant efforts to bring the bills to passage. We are thankful for your support and we are deploying those additional authorities with clarity of mission.

Additional legislation is needed. We must take additional steps to ensure that DHS is able to rapidly and efficiently deploy new protective technologies across Federal civilian agency information systems. In addition, carefully updating laws to facilitate cybersecurity information sharing within the private sector and between the private and government sectors is also essential to improving the Nation's cybersecurity. While many companies currently share cybersecurity threat information under existing laws, there is a heightening need to increase the volume and speed of information shared without sacrificing the trust of the American people or the protection of privacy, confidentiality, civil rights, or civil liberties. It is essential to ensure that cyber threat information can be shared quickly among trusted partners, including with law enforcement, so that network owners and operators can take necessary steps to block threats and avoid damage.

The NCCIC plays a critical role in the President's recent legislative proposal because its core mission – as articulated in the National Cybersecurity Protection Act, developed by this Committee and unanimously-passed by the House in December – is to coordinate and serve as an interface for cybersecurity information across the government and private sector.

The Administration's Information Sharing Proposal for Cyber Threat Indicators

Building on the bipartisan cybersecurity legislation enacted last Congress, President Obama visited the NCCIC on January 13, 2015, to announce a proposal for additional legislation to improve cybersecurity information sharing. The President noted, "Much of our critical infrastructure runs on networks connected to the Internet….[a]nd most of this infrastructure is owned and operated by the private sector. So neither government nor the private sector can defend the nation alone. It's going to have to be a shared mission – government and industry working hand in hand, as partners." This partnership entails sharing cyber threat indicators to better enable government agencies and the private sector to protect themselves.

Information sharing, especially of these technical "threat indicators" that can be used to identify and block malicious activity, is the lifeblood of effective cyber defense and response. Pulling together this information allows defenders to identify anomalies or patterns and recognize dangerous activity before it can do significant damage. The goal of the President's proposal is to increase the sharing of this type of information, as quickly as possible, with appropriate protection for privacy and of sensitive information and systems.

Among other things, the Administration's proposal would reduce the risks for private entities to voluntarily share technical cyber threat indicators with each other and the NCCIC by providing protections against civil or criminal liability for such sharing. Equally important, the proposal narrowly defines the threat indicators that will be shared, requires that irrelevant identifying information be minimized from these indicators, and generally requires strong protections for the privacy and confidentiality of personal information. Finally, the proposal calls for the creation of Information Sharing and Analysis Organizations (ISAOs). ISAOs would be information sharing organizations that would help speed information sharing within the private sector and between the private sector and government.

Our goal is to expand information sharing within the private sector, and to build on the existing relationships, processes and programs of the NCCIC to enhance cooperation between the government and private sector. The proposal will help us improve the methods that the NCCIC already uses to share cyber threat indicators, and leverage automation to achieve scalability wherever possible. We look to evolve and expand indicator sharing at the NCCIC from human exchanges, portals, and written reports to automated machine-to-machine communications. Our vision is that this may reduce the time to receive and act on indicators from hours to milliseconds, create consistency in information provided to interagency partners, law enforcement, and the private sector, and free analysts to focus on the threats that require human analysis while expediting detection and blocking of new threats.

NCCIC as the Coordination Center

Cyber threat indicators, which allow government agencies and the private sector to better protect themselves, come from a variety of sources, including: government agencies, private companies, international partners, and ISAOs. Given the variety of formats used – and information that is included – when sharing such information, the government must have a central clearinghouse to ensure that privacy and confidentiality protections are consistently applied and that the right information reaches the right government and private sector entities.

DHS is a leader within the government when it comes to the development and operational implementation of privacy, confidentiality, and civil liberties policies. DHS was the first agency to have statutorily established Officers for Privacy and for Civil Rights and Civil Liberties. From its creation, DHS has built both privacy and civil liberties protections into all of its programs and has dedicated, on-site privacy professionals committed to ensuring that its cyber mission is carried out in a way consistent with our Nation's values. Through statutory protections like Protected Critical Infrastructure Information (PCII), DHS will continue to anonymize the identity of submitters and other proprietary and sensitive information in threat indicator submissions. Moreover, the President's proposal calls for DHS to build upon its existing privacy, confidentiality, and civil liberty procedures by working with the

Attorney General to develop new procedures to appropriately limit Government receipt, use, and retention of threat indicators. Establishing the NCCIC as the primary entry way for cyber threat indicators from the private sector will ensure uniform application of these important privacy and confidentiality protections, while still allowing cyber threat indictors to be shared with law enforcement for the specific purposes identified in the legislation.

NCCIC sits at the intersection of cyber communities, with representatives from the private sector and other government entities physically present on the NCCIC floor and connected virtually. This diverse participation in the NCCIC was cemented by section 226(d) of the Homeland Security Act as added by the National Cybersecurity Protection Act. NCCIC's core mission is to enable better network defense by assessing and appropriately sharing information on the risks to America's critical cyber systems and how to reduce them.

Building Capacity to Accelerate Automated Sharing of Cyber Threat Indicators

The Administration's proposal directs DHS to automate and share information in as close to real-time as practicable with relevant federal agencies, including law enforcement entities, and with ISAOs. For the past three years, DHS has led the development in collaboration with the private sector of specifications – known as STIX and TAXII – which standardize the representation and exchange of cyber threat information, including actionable cyber threat indicators. STIX, the Structured Threat Information eXpression, is a standardized format for the representation and exchange of cyber threat information, including indicators. TAXII, the Trusted Automated eXchange of Indicator Information, is a standardized protocol for discovering and exchanging cyber threat information in STIX. The interagency Enhance Shared Situational Awareness initiative has already chosen STIX as the basis for sharing cyber threat indicators between the Federal cyber centers, ensuring interoperability between these key sources of information.

Through collaboration between DHS and the private sector, there is a solid and rapidly growing base of commercial offerings supporting STIX and sharing indicators via the TAXII, including platforms, network protection appliances and endpoint security tools. While the NCCIC has in-house systems and tools to assist analysts in generating STIX indicators, those indicators are currently analyzed and filtered by human analysts and shared back out with the private sector and Federal partners through manual methods such as e-mail and secure portals. In 2014, the NCCIC began a limited pilot with several organizations to test automated delivery of STIX indicators via TAXII.

To inform our plan for achieving automated cyber threat indicator information sharing, DHS created a working group between a range of DHS offices and the FBI, a critical stakeholder in the NCCIC. We also included experts from our Privacy, Civil Rights and Civil Liberties, and Science and Technology offices, among others, to ensure that our architecture is based on best-in-class technology and is consistent with our values and our respect for Americans' privacy and civil liberties.

Implementation will proceed through four major phases: (1) an initial operating capability phase in which we will deploy a TAXII system that can disseminate STIX cyber threat indicators with increased automation capability, enabling the use of human analysis for the most complex problems and egregious threats; (2) an expanded automation phase in which we will develop and deploy DHS infrastructure that can receive, filter, and analyze cyber threat indicators-- during this phase, we will

promulgate guidance for private sector companies to minimize, redact and tag their data prior to submission to NCCIC, and will complete a Privacy Impact Assessment; (3) a final operating capability phase in which we will fully automate DHS processes to receive and appropriately disseminate cyber threat indicators in a machine-readable format and finalize policies for filtering, receipt, retention, use, and sharing, including regular compliance reviews; and (4) a scaled services capability phase, during which DHS will work to enable agencies that lack sufficient cybersecurity resources or expertise to receive and share cyber threat indicators with the NCCIC in near-real-time by providing a turnkey technical solution to "plug in" to the NCCIC.

DHS Shares Information Widely with Federal Agencies and the Private Sector

Currently, DHS shares information with Federal Agencies and the private sector. DHS takes a customer-focused approach to information sharing, and different types of information require differing response times and dissemination protocols. DHS provides information to detect and block cybersecurity attacks on Federal civilian agencies and shares information to help critical infrastructure entities in their own protection; provides information to commercial cybersecurity companies so they can better protect their customers through the Enhanced Cybersecurity Services program, or ECS; and maintains a trusted information sharing environment for private sector partners to share information and collaborate on cybersecurity threats and trends via a program known as the Cyber Information Sharing and Collaboration Program, or CISCP. This trust derives in large part from our emphasis on privacy, confidentiality, civil rights, and civil liberties across all information sharing programs, including special care to safeguard personally identifiable information.

DHS also directly supports Federal civilian departments and agencies in developing capabilities that will improve their own cybersecurity posture. Through the Continuous Diagnostics and Mitigation (CDM) program, DHS enables Federal agencies to more readily identify network security issues, including unauthorized and unmanaged hardware and software; known vulnerabilities; weak configuration settings; and potential insider attacks. Agencies can then prioritize mitigation of these issues based upon potential consequences or likelihood of exploitation by adversaries. The CDM program provides diagnostic sensors, tools, and dashboards that provide situational awareness to individual agencies, and will provide DHS with summary data to understand relative and system risk across the Executive Branch. DHS is moving aggressively to implement CDM across all Federal civilian agencies, and Memoranda of Agreement with the CDM program encompass over 97 percent of all Federal civilian personnel.

While CDM will identify vulnerabilities and systemic risks within agency networks, the National Cybersecurity Protection System, also known as EINSTEIN, detects and blocks threats at the perimeter of those networks or at an agencies' Internet Service Provider. EINSTEIN is an integrated intrusion detection, analysis, information sharing, and intrusion-prevention system. The most recent iteration, Einstein 3 Accelerated (E3a), supplements EINSTEIN 2 by adding additional intrusion prevention capabilities and enabling Internet Service Providers (ISPs), under the direction of DHS, to detect and block known or suspected cyber threats using indicators.

Conclusion

We are working together to find new and better ways to share accurate, timely data in a manner

consistent with fundamental American values of privacy, confidentiality, and civil rights. While securing cyberspace has been identified as a core DHS mission since the 2010 Quadrennial Homeland Security Review, the Department's view of cybersecurity has evolved to include a more holistic emphasis on critical infrastructure which takes into account the convergence of cyber and physical risk.

Today our adversaries exploit a fundamental asymmetry in our network infrastructure: while nearly all of our systems and networks are globally interconnected, our defensive capabilities are not. This gives the attackers a compelling advantage as they can find and exploit the weak links in our systems from anywhere around the world – at machine speed. By sharing cyber threat indicators in near real-time, we reduce that asymmetry.

As our defensive cybersecurity capabilities become more interconnected, we greatly reduce the likelihood that an adversary can re-use attack infrastructure, tools, tactics, techniques and procedures. In addition, we greatly reduce the time window in which new and novel attacks are effective because the ecosystem shares those indicators and develops a type of "herd immunity," improving defenses as indicators are shared and events are correlated in near-real-time. These two factors do not eliminate all cyber threats, but they hold the promise of significantly increasing the time and resources (both technical and human) that attackers must expend to achieve their goals. Moreover, the STIX data format and the TAXII transport method are increasingly compatible with commonly used commercial information technology (IT) products. This means more entities are able to send indicators automatically to the NCCIC, creating an ecosystem of indicators which will in turn provide greater context to malicious cyber activity and rapidly increase situational awareness per Executive Order 13636, *Improving Critical Infrastructure Cybersecurity* and Executive Order 13691, signed February 13, 2015, *Promoting Private Sector Cybersecurity Information Sharing*.

DHS will continue to serve as one of the government's primary resources for information sharing and collaborative analysis, at machine-speed wherever possible, of global cyber risks, trends, and incidents. Through our leadership role in protecting civilian government systems and helping the private sector protect itself, DHS can correlate data from diverse sources, in an anonymized and secure manner, to maximize insights and inform effective risk mitigation.

DHS provides the foundation of the U.S. government's approach to securing and ensuring the resilience of civilian critical infrastructure and essential services. We look forward to continuing the conversation and supporting the American goals of peace and stability; in these endeavors, we rely upon your continued support.

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

Congressional Research Service

Statement of Eric A. Fischer
Senior Specialist in Science and Technology
Congressional Research Service

Before

Committee on Homeland Security
U.S. House of Representatives

February 25, 2015

on

"Examining the President's Cybersecurity Information Sharing Proposal"

Chairman McCaul, Ranking Member Thompson, and distinguished Members of the Committee:

Thank you for this opportunity to discuss legislative proposals on information sharing in cybersecurity.[1] In January of this year, the White House announced a revision of its 2011 information-sharing proposal as part of a set of updated proposals and other actions relating to cybersecurity:[2]

- A draft bill to enhance information sharing on cybersecurity within the private sector and between the private sector and the federal government. Most of my testimony today will focus on this proposal and related bills in the 113th and 114th Congresses.[3]
- A draft bill to amend federal statutes relating to cybercrime by creating or increasing criminal penalties for certain types of offenses and providing some other authorities to law-enforcement agencies and the courts.[4]

[1] This statement is limited to a policy analysis of the proposals and initiatives discussed and is not intended to reach any legal conclusions regarding them.

[2] The White House, "Securing Cyberspace: President Obama Announces New Cybersecurity Legislative Proposal and Other Cybersecurity Efforts," Press Release (January 13, 2015), http://www.whitehouse.gov/the-press-office/2015/01/13/securing-cyberspace-president-obama-announces-new-cybersecurity-legislat.

[3] The White House, *Updated Information Sharing Legislative Proposal*, 2015, http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/updated-information-sharing-legislative-proposal.pdf.

- A draft bill to harmonize state laws requiring companies holding personal information on customers to notify them of data breaches involving such information.[5]
- A five-year, $25 million grant to create a new cybersecurity consortium consisting of 13 Historically Black Colleges and Universities (HBCUs), the Lawrence Livermore and Sandia National Laboratories of the Department of Energy, and a South Carolina school district. The object of the program is to help fill demand for cybersecurity professionals while diversifying the pipeline of talent for this and related fields of expertise.[6] This program can be seen as a complement to legislation enacted by the 113th Congress that addresses cybersecurity workforce needs in the Department of Homeland Security[7] (DHS) and more broadly.[8]

The announcement also included a description of the White House cybersecurity summit held on February 13 at Stanford University.

Barriers to the sharing of information on threats, attacks, vulnerabilities, and other aspects of cybersecurity—both within and across sectors—have long been considered by many to be a significant hindrance to effective protection of information systems, especially those associated with critical infrastructure.[9] Examples have included legal barriers, concerns about liability and misuse, protection of trade secrets and other proprietary business information, and institutional and cultural factors—for example, the traditional approach to security tends to emphasize secrecy and confidentiality, which would necessarily impede sharing of information.

---

[4] The White House, *Updated Administration Proposal: Law Enforcement Provisions*, 2015, http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/updated-law-enforcement-tools.pdf.

[5] The White House, *The Personal Data Notification & Protection Act*, 2015, http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/updated-data-breach-notification.pdf.

[6] The White House, "Vice President Biden Announces $25 Million in Funding for Cybersecurity Education at HBCUs," Press Release (January 15, 2015), http://www.whitehouse.gov/the-press-office/2015/01/15/vice-president-biden-announces-25-million-funding-cybersecurity-educatio.

[7] H.R. 2952, the Cybersecurity Workforce Assessment Act (P.L. 113-246), and S. 1691, the Border Patrol Agent Pay Reform Act of 2014 (P.L. 113-277), requiring assessments of workforce needs within the Department of Homeland Security and providing enhanced authorities to the Secretary for recruitment and retention of cybersecurity personnel.

[8] S. 1353, the Cybersecurity Enhancement Act of 2014 (P.L. 113-274), establishing in statute a National Science Foundation program for educating cybersecurity professionals for government agencies, and an interagency program of challenges and competitions in cybersecurity to stimulate identification and recruitment of cybersecurity professionals more broadly as well as cybersecurity research and innovation.

[9] See, for example, The Markle Foundation Task Force on National Security in the Information Age, *Nation At Risk: Policy Makers Need Better Information to Protect the Country*, March 2009, http://www.markle.org/downloadable_assets/20090304_mtf_report.pdf; CSIS Commission on Cybersecurity for the 44th Presidency, *Cybersecurity Two Years Later*, January 2011, http://csis.org/files/publication/110128_Lewis_CybersecurityTwoYearsLater_Web.pdf.

A few sectors are subject to federal notification requirements,[10] but most such information sharing is voluntary, often through sector-specific Information Sharing and Analysis Centers (ISACs)[11] or programs under the auspices of the Department of Homeland Security (DHS) or sector-specific agencies.[12]

While there is some disagreement among experts about whether federal legislation is needed to address the problem, there appears to be fairly broad consensus that such legislation could be useful if crafted appropriately but potentially harmful if not. However, there is disagreement about what the key characteristics of useful legislation would be. Proposals to reduce or remove such barriers, including provisions in legislative proposals in the last two Congresses, have raised concerns, some of which are related to the purpose of barriers that currently impede sharing. Examples include risks to individual privacy and even free speech and other rights, use of information for purposes other than cybersecurity, such as unrelated government regulatory actions, commercial exploitation of personal information, or anticompetitive collusion among businesses that would currently violate federal law.

More broadly, debate has tended to focus on questions such as the following:

1. What are the kinds of information for which barriers to sharing exist that make effective cybersecurity more difficult, and what are those barriers?
2. How should information sharing be structured in the public and private sectors to ensure that it is efficient and effective?
3. What are the risks to privacy rights and civil liberties of individual citizens associated with sharing different kinds of cybersecurity information, and how can those rights and liberties best be protected?
4. What, if any, statutory protections against liability are needed to reduce disincentives for private-sector entities to share cybersecurity information with each other and with government agencies, and how can the need to reduce such barriers best be balanced against any risks to well-established protections?
5. What improvements to current standards and practices are needed to ensure that information sharing is useful and efficient for protecting information systems, networks, and their contents?

---

[10] Notable examples include the chemical industry, electricity, financial, and transportation sectors.

[11] See, for example, ISAC Council, "National Council of ISACS," 2015, http://www.isaccouncil.org/. ISACs were originally formed pursuant to a 1998 presidential directive (The White House, "Presidential Decision Directive 63: Critical Infrastructure Protection," May 22, 1998, http://www.fas.org/irp/offdocs/pdd/pdd-63.htm).

[12] See also CRS Report R42114, *Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions*, by Eric A. Fischer; CRS Report R42409, *Cybersecurity: Selected Legal Issues*, by Edward C. Liu et al.; CRS Report R42984, *The 2013 Cybersecurity Executive Order: Overview and Considerations for Congress*, by Eric A. Fischer et al.; CRS Report R4381, *Legislation to Facilitate Cybersecurity Information Sharing: Economic Analysis*, by N. Eric Weiss.

The White House information sharing proposal would attempt to address such questions in several ways. The discussion below includes a summary of how the proposal would address them in comparison to the following bills addressing information sharing:

- H.R. 234, the Cyber Intelligence Sharing and Protection Act (CISPA), in the 114th Congress, identical to H.R. 624 as passed by the House in the 113th Congress;
- S. 2588, Cybersecurity Information Sharing Act of 2014 (CISA) as reported to the Senate in the 113th Congress;
- S. 456, the Cyber Threat Sharing Act of 2015, as introduced in the 114th Congress.

Kinds of Information Shared

Information sharing can involve a wide variety of material communicated on a wide range of timescales, ranging from broad cybersecurity policies and principles to best practices to descriptions of specific threats and vulnerabilities to computer-generated data transmitted directly from one information system to another electronically. The level of sensitivity of information can also vary—for example, it may be classified, proprietary, or personal. Information of any class will also vary in its value for cybersecurity and the degree to which it needs human processing to be useful.[13]

To the extent that the goal of information sharing is to defend information systems against cyberattacks, there appears to be a consensus that shared information needs to be actionable—that is, it should identify or evoke a specific response aimed at mitigating cybersecurity risks. To be meaningfully actionable, information may often need to be shared very quickly or even in an automated fashion. There may therefore be little or no time for human operators to examine a specific parcel of data to determine whether sharing it could raise privacy, liability, or other concerns.

The White House proposal would limit the scope of shared information covered under the proposal to "cyber threat indicators," which includes information needed to "indicate, describe, or identify" malicious reconnaissance or command and control activities, methods of social engineering and of defeating technical or operational controls, and technical vulnerabilities, and from which "reasonable efforts" have been made to remove personally identifying information if the person is thought to be unrelated to the threat. The definition in S. 456 is largely identical.

The definition in the White House proposal and S. 456 are arguably the narrowest in scope. S. 2588 also focuses on "cyber threat indicators," with a definition that is similar to that in the White House proposal, but is somewhat broader, including other attributes, such as the actual or potential harm caused by an incident. It also expressly permits sharing of information on countermeasures—measures to prevent or mitigate threats and vulnerabilities.

H.R. 234 uses the term "cyber threat information," characterized as information "directly pertaining to" efforts to gain unauthorized access to information systems or to effect negative impacts on systems or networks, threats to the information security of a system or its contents,

[13] See, for example, Kathleen M. Moriarty, "Transforming Expectations for Threat-Intelligence Sharing," *RSA Perspective* (August 3, 2013), https://www.emc.com/collateral/emc-perspective/h12175-transf-expect-for-threat-intell-sharing.pdf.

and vulnerabilities of systems and networks. The bill also defines a related term, "cyber threat intelligence," with characteristics similar to those of cyber threat information but is in the possession of the Intelligence Community.

Structure of Information Sharing

Information sharing can conceivably lead to information overload, where an entity receives much more information than it can reasonably process. That could include not only information of uncertain quality and use, but also similar or redundant information from a variety of sources. In addition, a proliferation of sharing mechanisms could lead to stovepiping, which could reduce sharing across sectors, for example, and lack of clarity with respect to responsibilities, which could lead to gaps in sharing useful information. In contrast, a narrow, tightly defined structure for information sharing could lead to logjams or impede innovation in response to continuing evolution of cyberspace.

The White House proposal and S. 456 would create a structure for information sharing that includes the National Cybersecurity and Communications Integration Center (NCCIC) as the federal hub for receipt and distribution of cybersecurity information, and fostering the use of private information sharing and analysis organizations (ISAOs) as recipients of information from private entities.[14] ISAOs could presumably also share such information under the provisions of the Homeland Security Act, but the proposal does not specifically address that function for them. The proposal would require the DHS Secretary to ensure that indicators are shared in a timely fashion with other federal agencies. S. 456 would require that procedures for such sharing be established and would specifically require the Secretary to ensure that both useful classified and unclassified information is shared with nonfederal entities.

H.R. 234 would create an entity at DHS (presumably the NCCIC[15]) to share threat information and an entity at the Department of Justice to share cybercrime information. It would require individual agencies that receive threat information to develop procedures for sharing it. In contrast to S. 456, it would require the Director of National Intelligence to establish procedures for sharing classified threat information. It would also designate specific classes of private-sector entities as those permitted to monitor systems and share threat information under the bill. Those include entities that provide cybersecurity goods and services to others or to themselves.

S. 2588 would require DHS to create a "capability and process" for sharing both threat indicators and countermeasures. It would establish an interagency process to develop procedures for

---

[14] ISAOs were defined in the Homeland Security Act (6 U.S.C. §131(5)) as entities that gather and analyze information relating to the security of critical infrastructure, communicate such information to help with defense against and recovery from incidents, and disseminate such information to any entities that might assist in carrying out those goals. The proposal covers receipt of indicators by ISAOs but does not mention communication or dissemination of information by them, except, by inference, to the NCCIC. Information Sharing and Analysis Centers (ISACs) are more familiar to most observers. They may also be ISAOs but are not the same, having been originally formed pursuant to a 1998 presidential directive (The White House, "Presidential Decision Directive 63: Critical Infrastructure Protection," May 22, 1998, http://www.fas.org/irp/offdocs/pdd/pdd-63.htm).

[15] The text in the bill was originally drafted before the enactment of the National Cybersecurity and Communications Integration Center Act of 2014 (P.L. 113-282), which established the NCCIC by statute.

sharing federal information with the private sector. It would require development of an interagency process for sharing classified threat indicators.

Timeliness of Sharing

The timescale on which shared information will be most useful varies. That is especially an issue in an environment where the relevance of timing for shared information may be measured in seconds or even milliseconds in many cases.[16] The White House proposal and S. 456 would address this concern by requiring the NCCIC to share indicators "in as close to real time as practicable" and by requiring establishment of a program to advance automated mechanisms for such sharing.

H.R. 234 and S. 2588 would also require "real-time sharing." The meaning of this term is not explicitly defined or described in the bills, but it presumably refers to sharing that occurs rapidly, for example, by machine-to-machine transmission. That is consistent with the stated purposes of the legislative proposals, in that threat information would likely need to be disseminated quickly in order to detect or prevent incoming cyberattacks, which can occur very quickly. This raises the question of whether this term should require any particular mode of sharing, for example, by machine-to-machine transmission without or with minimal intervening processing by human operators, and how different interpretations of the term may impact operational effectiveness, privacy interests, and competition for technical and financial resources. The White House proposal appears to address that through its proposed development of automated mechanisms, and S. 2588 would require development of a process to receive indicators and countermeasures electronically, including via an "automated process between information systems."

Privacy and Civil Liberties

Concerns relating to privacy and civil liberties, especially the protection of personal and proprietary information and uses of shared information, have been a significant source of controversy in debate about information sharing legislation. Such concerns have arisen in part because the White House proposal and the bills would permit sharing of specified cybersecurity information by covered private entities "notwithstanding any other provision of law." That would arguably remove barriers to sharing stemming from concerns that information would inadvertently violate laws such as those on privacy and antitrust.

However, it also raises concerns about privacy and civil liberties. In particular, personally identifying information might be included in the shared information but might not be related to the threat. In addition, data analytics might conceivably be used to draw inferences about identity from data sets even if any given piece of the shared information would not be identifying. Second, if access to shared information is not strictly controlled and restricted, or is used for purposes other than cybersecurity, risks to civil liberties may arise. Concerns have also been raised about regulatory use of shared information and disclosure of proprietary business information.

The White House proposal would address such concerns by

---

[16] See, for example, M.J. Herring and K.D. Willett, "Active Cyber Defense: A Vision for Real-Time Cyber Defense," *Journal of Information Warfare* 13, no. 2 (April 2014): 46–55.

- limiting application of the "notwithstanding" provision to indicators disclosed to the NCCIC and ISAOs;
- limiting private-sector use of shared indicators to purposes relating to protection of information systems and their contents;
- requiring minimization of personally identifiable information and safeguarding of any such information that cannot be removed;
- requiring development of guidelines by the Attorney General on limiting the acquisition and sharing of personally identifiable information and establishing processes for anonymization, safeguarding, and destruction of information;
- exempting information received by the federal government from disclosure under the Freedom of Information Act;
- prohibiting use of shared information for regulatory enforcement;
- requiring penalties for federal violations of its restrictions relating to information sharing; and
- an annual report to Congress on privacy and civil liberties.

S. 456 includes those provisions but would also permit a private entity to receive indicators under the "notwithstanding" provision.

H.R. 234 and S. 2588 have related provisions except as follows: Both bills explicitly limit federal use of shared information to cybersecurity purposes and uses relating to protection of individuals and investigation and prosecution of cybercrimes and certain other offenses. They both require various activities to reduce the degree to which personal information is shared and other means of safeguarding it from unauthorized sharing and use. H.R. 234 requires that guidelines be developed through an interagency process.

Liability Protections

Concern about liability has often been cited as a significant barrier to private-sector sharing of cybersecurity information, both with other private entities and with the federal government. In addition to the protections granted by the use of "notwithstanding any other provision of law" with respect to provision of information by private-sector entities, the White House proposal would address this issue by prohibiting civil or criminal actions in federal or state courts for covered activities with respect to lawfully obtained cyberthreat indicators disclosed to or received from the NCCIC or a certified ISAO. However, it also specifies monopolistic actions such as price-fixing that are not permitted.

The prohibition on civil or criminal actions in H.R. 234 covers acquisition and sharing of cyberthreat information, or decisions for cybersecurity purposes based on such information. The bill stipulates that actions must be taken in good faith. The S. 2588 prohibition covers only private defendants, and includes monitoring systems or sharing information. S. 2588 states that a good-faith reliance that an activity was permitted under the bill's provisions will serve as a complete defense against any court action. It also stipulates that private-sector exchange of cyberthreat information or assistance for cybersecurity purposes does not violate antitrust laws, but further specifies monopolistic actions such as price-fixing that are not permitted.

Improvements to Standards and Practices

The concerns discussed above about what information would be most useful to share and how raise the question of whether better standards and best practices are needed for improving the effectiveness and efficiency of information sharing.[17] The White House proposal and S. 456 would require the DHS Secretary to establish a process for selecting a private entity that would determine best practices for creating and operating private ISAOs. The recent executive order on information sharing has a similar provision.[18] There are no similar provisions in the other bills.

[17] See, for example, Moriarty, *Transforming Expectations for Threat-Intelligence Sharing*.

[18] Executive Order 13691, "Promoting Private Sector Cybersecurity Information Sharing," *Federal Register* 80, no. 34 (February 20, 2015): 9349–53.