Deputy Secretary
U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

July 31, 2015

The Honorable Al Franken
Ranking Member
Subcommittee on Privacy,
Technology, and the Law
Committee on the Judiciary
United States Senate
Washington, DC 20510

Dear Senator Franken:

Thank you for your July 1, 2015 letter. Secretary Johnson asked that I respond on his behalf.

Recent legislation codifies the authorities of the U.S. Department of Homeland Security to effectively lead efforts to protect the federal civilian executive branch's information technology systems from cyber-attack. Additionally, the Department's National Cybersecurity and Communications Integration Center is codified as the central hub for working voluntarily with federal and non-federal entities.

The Department has moved forward urgently in expanding the breadth and speed of our cybersecurity information sharing while ensuring appropriate protections for privacy, civil rights, and civil liberties. Of particular note, we now share cyber threat indicators at machine speed with a pilot group of participants, subject to appropriate privacy guidelines, and expect to begin sharing with and receiving from additional agencies and companies by this fall. We take privacy interests seriously and account for them at all stages of our cybersecurity work.

We appreciate the opportunity to further discuss the elements of the Cybersecurity Information Sharing Act. The attached enclosure contains detailed responses to your questions.

Thank you for your letter and interest in this matter. Should you require additional assistance, please do not hesitate to contact me at 202-282-8204.

Sincerely,

Alejandro N. Mayorkas

Enclosure

The U.S. Department of Homeland Security's Response to Senator Franken's July 1, 2015 letter

1. ***In what ways do private entities currently share with, and receive from, the government cyber threat information? How is information shared among government entities or with representatives of various government entities?***

Information sharing must be tailored to the particular requirements of the recipient organization and reflective of the various types and uses of cybersecurity information. To this end, the Department of Homeland Security (DHS) National Protection and Programs Directorate (NPPD) engages in information sharing with government and private sector partners in five primary ways:

- In-person information sharing on the National Cybersecurity and Communications Integration Center (NCCIC) watch floor;
- Bilateral sharing of cyber threat indicators, including via the Cyber Information Sharing and Collaboration Program (CISCP) and through automated sharing and receipt of cyber threat indicators;
- As-needed information sharing via standing groups;
- Broad dissemination of alerts and bulletins;
- Strategic engagement and collaboration.

Real-Time Collaboration on the NCCIC Watch Floor

The NCCIC, as codified by the National Cybersecurity Protection Act of 2014, serves as a central hub for cybersecurity information sharing between federal agencies, the private sector, law enforcement, and the intelligence community. Through a watch floor that operates twenty-four hours a day, seven days a week, the NCCIC provides a forum for real-time collaboration to understand and gain situational awareness of cybersecurity incidents and risks. Currently, representatives of several federal agencies (U.S. Northern Command, U.S. Cyber Command, National Security Agency, U.S. Secret Service, U.S. Immigration and Customers Enforcement, U.S. Department of the Treasury, the Department of Justice's Federal Bureau of Investigation, and the U.S. Department of Energy) and four Information Sharing and Analysis Centers , which represent the financial, aviation, and energy sectors as well as state, local, tribal, and territorial governments, have dedicated liaisons on the NCCIC watch floor. Further, 114 private sector companies have as-needed access to the NCCIC through their participation in CISCP. Federal agencies with cleared personnel maintain similar as-needed access.

Bi-Directional Sharing of Cyber Threat Indicators

A key element of DHS's information sharing approach for public and private partners is to share cyber threat indicators widely and at machine speed in formats that can be

immediately used for network defense.[1] Our goal is thus to broaden the base and increase the speed of information sharing to help ensure that an adversary can only use a given attack one time before it is blocked by all other government and private sector partners–increasing the attacker's costs and reducing the prevalence of damaging cybersecurity incidents.

CISCP is the Department's flagship program for public-private information sharing. CISCP provides a platform and a trusted forum for exchanging threat and vulnerability information, governed by a Cooperative Research and Development Agreement (CRADA) between DHS and each CISCP participant. The CRADA allows participants to gain as-needed access to the NCCIC, a mechanism to receive security clearances, and the ability to participate in bi-directional information sharing. Currently, information sharing in CISCP is conducted via secure e-mail or an online portal.

Moving forward, DHS is beginning to share "machine-readable" cyber threat indicators automatically and in near-real time automated indicator sharing. Automated indicator sharing uses the DHS-developed STIX/TAXII formats, a mechanism for sharing cyber threat information in a common manner. STIX/TAXII allows public and private sector partners to share cyber threat information in the same way so that computers can immediately use the information for network defense. Cybersecurity vendors are now integrating STIX/TAXII into their commercial products, further broadening use of the standard. DHS is already using this initiative to send out uni-directionally, machine-readable cyber threat indicators at near-real-time to one government agency. We are working to expand recipients across the public and private sectors.

DHS reviews all cyber threat indicators for privacy, civil liberties and other compliance concerns. Currently, these reviews are conducted by human analysis. With automated indicator sharing, we will continue to review all indicators, but will transition to rely substantially on a rules-based approach that combines automated and human review. This will ensure that all privacy, civil liberties, and other compliance concerns are proactively identified and mitigated while minimizing time delays and resource requirements currently associated with such analysis.

Today, DHS is sharing cyber threat indicators with an initial set of partners and is in the process of adding additional companies, Information Sharing and Analysis Organizations (ISAOs), and Federal agencies.[2] Later this year, DHS will begin to accept cyber threat

[1] A malicious email address or Internet Protocol (IP) address are two examples of cyber threat indicators.
[2] As provided by Executive Order 13691, ISAOs are "intended to enable and facilitate private companies, nonprofit organizations, and executive departments and agencies …to share information related to cybersecurity risks and incidents and collaborate to respond in as close to real time as possible." DHS will enter into an agreement with a nongovernmental organization to identify a common set of voluntary best practices for the creation and functioning of ISAOs in the fourth quarter of fiscal year 2015.

indicators from the private sector via STIX and TAXII and automate the processes required for protecting, minimizing, and redacting sensitive information. Companies participating in CISCP are expected to be the first participants in automated information sharing, via an addendum to their current CISCP CRADA. DHS expects to begin bidirectional information sharing (dissemination and receipt) with private sector companies by this fall.

Standing Information Sharing Groups

During a cybersecurity incident or in response to an exigent risk, it is essential to convene appropriate entities to quickly share information and promulgate necessary mitigations. For the federal civilian executive branch, such collaboration occurs via two mechanisms. First, the NCCIC maintains direct information sharing relationships with the Security Operations Centers (SOCs) of all federal agencies. Communication with the SOCs occurs both in the steady-State, via regular update calls, and as needed in response to significant incidents or emergent risks. This direct relationship with the SOCs is essential to rapidly communicate technical information and gain a deep understanding of operational issues at specific agencies or across the federal government. Second, the NCCIC convenes Cyber Collaboration, Assessment, and Response (C-CAR) calls with agency Chief Information Officers (CIOs) or agency Chief Information Security Officers (CISOs). C-CAR calls ensure that agency CIOs and CISOs are empowered with the necessary information to drive critical detection or mitigation activities across their agencies and provide DHS with the information necessary to understand government-wide risk.

With the private sector, the NCCIC shares emergent information via the Cyber Unified Coordination Group (UGC). The UCG consists of senior representatives from key federal agencies, major companies across critical infrastructure sectors, and state, local, tribal, and territorial governments. During a significant incident, the UCG is the principal mechanism to collaborate with key private sector partners in a secure forum and plan integrated responses that appropriately incorporate priorities from the government and private sector.

Cybersecurity Alerts, Bulletins, and Other Messages

The NCCIC develops and disseminates alerts and bulletins via e-mail to particular distribution lists (such as federal Security Operations Centers, state, local, tribal, and territorial governments, and international partners), on public websites, and through secure online portals. These alerts and bulletins provide detailed technical guidance and context that security professionals use to both understand the particular risk and implement effective mitigations. In fiscal year 2014, the NCCIC disseminated nearly 12,000 alerts, bulletins, and other products to approximately 100,000 recipients.

Strategic Engagement and Collaboration

Finally, NPPD convenes partners to understand cybersecurity risks and share best practices. Through fora such as Advanced Threat Technical Exchanges that bring together cross-sector companies participating in CISCP, such collaboration also helps participating organizations gain deep context into the intricacies of specific cybersecurity risks. As the Sector-Specific Agency for the Information Technology and Communications sectors and the federal government's lead for critical infrastructure protection, NPPD serves a key role as a convening organization between the public and private sectors. With its government partners, NPPD leverages CyberStats, CIO Interviews, and an *ex oficio* role on the Federal CIO Council to conduct similar strategic engagement and ensure a recognition of cybersecurity risks among agency CIOs and management executives.

2. ***What kinds of concerns does it raise, in your view, to have legislation that newly authorizes, and thus may encourage, information sharing with other agencies, and not through the NCCIC?***

While the Cybersecurity Information Sharing Act seeks to incentivize non-federal sharing through a DHS portal, the bill's authorization to share with any federal agency "notwithstanding any other provision law" undermines that policy goal, and will increase the complexity and difficulty of a new information sharing program.

The President's January 2015 cybersecurity information sharing proposal contemplates that all cybersecurity threat indicators shared with the government would be shared through the NCCIC, a non-law enforcement, non-intelligence center focused on network defense activities. Permitting sharing directly with law enforcement and intelligence entities will be of significant concern to the privacy and civil liberties communities.

The authorization to share cyber threat indicators and defensive measures with "any other entity or the Federal Government," "notwithstanding any other provision of law" could sweep away important privacy protections, particularly the provisions in the Stored Communications Act limiting the disclosure of the content of electronic communications to the government by certain providers. (This concern is heightened by the expansive definitions of cyber threat indicators and defensive measures in the bill. Unlike the President's proposal, the Senate bill includes "any other attribute of a cybersecurity threat" within its definition of cyber threat indicator and authorizes entities to employ defensive measures.)

The Administration has consistently maintained that a civilian entity, rather than a military or intelligence agency, should lead the sharing of cyber threat indicators and defensive measures with the private sector. *The National Cybersecurity Protection Act of 2014* recognized the NCCIC to be responsible for coordinating the sharing of information

related to cybersecurity risks and to be the federal civilian interface for multi-directional and cross-sector sharing of information about cybersecurity risks and warnings. The NCCIC has representatives from the private sector and other federal entities involved in cyber information sharing, from those with whom we have an agreement and share consistently, to those that passively receive information from the center.

Equally important, if cyber threat indicators are distributed amongst multiple agencies rather than initially provided through one entity, the complexity–for both government and businesses–and inefficiency of any information sharing program will markedly increase; developing a single, comprehensive picture of the range of cyber threats faced daily will become more difficult. This will limit the ability of DHS to connect the dots and proactively recognize emerging risks and help private and public organizations implement effective mitigations to reduce the likelihood of damaging incidents.

DHS recommends limiting the provision in the Cybersecurity Information Sharing Act regarding authorization to share information, notwithstanding any other provision of law, to sharing through the DHS capability housed in the NCCIC. This would not preclude sharing with any federal entity (indeed, DHS maintains an obligation to share rapidly with federal partners independent of any legislation), and it would further incentivize sharing through the NCCIC.

3. ***I am concerned that the Senate Intelligence Committee's bill falls short with regard to privacy protections. I do not believe it imposes a sufficiently stringent standard for the removal of irrelevant personally identifiable information, and seems to fall short of the privacy-protective standards DHS has set for itself. Moreover, the bill's requirement that DHS share the cyber threat information it receives through a designated electronic capability with other agencies in "real time" and without modification is at odds with ensuring that DHS can continue to carry out its current, privacy-protective protocols or can fully comply with privacy guidelines imposed under the bill. Please address the importance of DHS's current policies and protocols for the removal and minimization of PII in cyber threat information that the agency collects or receives from private entities.***

We share your concern that sharing cyber threat information "not subject to any delay [or] modification" raises privacy and civil liberties concerns and would complicate efforts to establish an automatic sharing regime.

To require sharing in "real time" and "not subject to any delay [or] modification" raises concerns relating to operational analysis and privacy.

First, it is important for the NCCIC to be able to apply a privacy scrub to incoming data, to ensure that personally identifiable information unrelated to a cyber threat has not been included. If DHS distributes information that is not scrubbed for privacy concerns, DHS

would fail to mitigate and in fact would contribute to the compromise of personally identifiable information by spreading it further. While DHS aims to conduct a privacy scrub quickly so that data can be shared in close to real time, the language as currently written would complicate efforts to do so. DHS needs to apply business rules, workflows and data labeling (potentially masking data depending on the receiver) to avoid this problem.

Second, customers may receive more information than they are capable of handling, and are likely to receive large amounts of unnecessary information. If there is no layer of screening for accuracy, DHS' customers may receive large amounts of information with dubious value, and may not have the capability to meaningfully digest that information.

While the current Cybersecurity Information Sharing Act recognizes the need for policies and procedures governing automatic information sharing, those policies and procedures would not effectively mitigate these issues if the requirement to share "not subject to any delay [or] modification" remains.

To ensure automated information sharing works in practice, DHS recommends requiring cyber threat information received by DHS to be provided to other federal agencies in "as close to real time as practicable" and "in accordance with applicable policies and procedures."

4. ***What concerns does the bill, as introduced in the Senate, raise in DHS's view? In particular, please address the operational effectiveness and efficiency of the information sharing called for by the bill.***

As highlighted in our answers to questions 2 and 3, we have concerns with a bill that permits sharing with agencies other than DHS "notwithstanding any other provision of law," and that mandates real-time dissemination of indicators without delay or modification. These provisions would undermine the policy goals that were thoughtfully constructed to maximize privacy and accuracy of information, and to provide the NCCIC with the situational awareness we need to better serve the nation's cybersecurity needs.

Additionally, we have several other concerns with the bill as written. First, the provision that permits entities to designate information provided to the federal government as "proprietary" could be too restrictive. These protections (in Section 5(d)(2)) may deprive numerous private sector entities of a valuable source of cyber threat information helpful for network defense activities. This is because the provision might be read to limit DHS's ability to share this information with other non-federal entities. We therefore recommend that section 5(d)(2) be edited to clarify that information is not proprietary once anonymized to remove any reference to the identity of the submitting entity.

When DHS receives cyber threat information from the private sector today—including information that is protected from disclosure as Protected Critical Infrastructure Information—it routinely anonymizes such information by removing any reference to the entity submitting the information and shares the anonymized cyber threat information with other private entities. Private sector submitters of information to DHS have not expressed concerns with this approach, which both protects the identity of the submitter and enables other entities to use the information to protect themselves. While cyber threat information shared by the private sector can be viewed as proprietary in its original form, anonymized threat information should not be viewed as proprietary in a sense that would limit appropriate sharing.

Second, we believe that DHS should be the primary author of the policies and procedures under sections 3 and 5 (especially 5(a)). Since sharing cyber threat information with the private sector is primarily within DHS's mission space, DHS should author the section 3 procedures, in coordination with other entities. In addition, the scope of the Attorney General's policies and procedures outlined in the Cybersecurity Information Sharing Act is problematic. Because DHS will be operating the federal government's capability to receive cyber threat information under section 5(c), it is not feasible for another agency to issue the procedures that will govern the day-to-day operations of such a capability. We recommend that DHS be assigned the responsibility to issue policies and procedures under section 5(a), and be listed as a co-author of the procedures under section 5(b).

Third, we strongly support the EINSTEIN amendment that was added to the House of Representatives bill, which authorizes DHS capabilities to protect federal civilian agency information systems. We would seek to make one change in that language, however. The language in Section (b)(3), "only to protect federal agency information and information systems from cybersecurity risks," is too narrow, as we also share malware/indicators found in federal communications with the private sector to protect their information systems. We recommend replacing the phrase with "only for cybersecurity purposes" or deleting "federal agency."

Finally the 90-day timeline for DHS's deployment of a process and capability to receive cyber threat indicators is too ambitious, in light of the need to fully evaluate the requirements pertaining to that capability once legislation passes and build and deploy the technology. At a minimum, the timeframe should be doubled to 180 days.