WRITTEN STATEMENT OF MARY ELLEN CALLAHAN
Partner and Chair, Privacy and Information Governance Practice, Jenner & Block
Former Chief Privacy Officer, U.S. Department of Homeland Security

Before the House Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies

INDUSTRY PERSPECTIVES ON THE PRESIDENT'S CYBERSECURITY INFORMATION SHARING PROPOSAL

March 4, 2015 Hearing

Chairman Ratcliffe, Ranking Member Richmond, Distinguished Members of the Subcommittee, thank you for the opportunity to appear before you today. My name is Mary Ellen Callahan. I am a partner at the law firm of Jenner & Block, where I chair the Privacy and Information Governance Practice and counsel private-sector clients on integrating privacy and cybersecurity. From March 2009 to August 2012, I served as the Chief Privacy Officer at the U.S. Department of Homeland Security (DHS or Department). I have worked as a privacy professional for 17 years and have national and international experience in integrating privacy into business and government operations. I am appearing before this subcommittee in my personal capacity and not on behalf of any other entity.

Cybersecurity information sharing is vital to protect the private and public sector assets. In order to prepare for disclosing cybersecurity threat indicators to other entities in the cybersecurity ecosystem, however, the information sharing with the government must meet certain standards to address industry interests and needs.

In my testimony, I will address six factors that are crucial to establishing robust, effective private sector information sharing with the government. First and foremost, to encourage and facilitate private sector information sharing, the government must develop and implement legitimate privacy safeguards. Second, clearly established controls must be placed on what the government does with the shared information. Third, those controls must include identifying and empowering a civilian interface with the private sector on information sharing – not just as an intake center, but for all communications related to cybersecurity information sharing. The fourth necessary step is to establish the value proposition for information sharing; information sharing must be at an acceptable cost and provide minimal risk for the participants. Its companion point is to define clear and objective limitations on liability for companies that participate in information sharing – both civilly and criminally. And finally, Congress should expressly provide the Privacy and Civil Liberties Oversight Board with oversight authority over cybersecurity, including information sharing.

Privacy Safeguards are Essential to Effective Private Sector Information Sharing

As Apple CEO Tim Cook noted at the Cybersecurity Summit last month, we have to protect our privacy rights or we will all face dire consequences. At the same Summit, President Obama concurred, saying, "When people go online, we shouldn't have to forfeit the basic privacy we're

entitled to as Americans." However, the *Executive Order on Promoting Private Sector Cybersecurity Information Sharing* does not include a comprehensive privacy and civil liberties framework relating to private sector sharing, instead focusing only on the intra-government sharing, instructing agencies to work with their Senior Agency Officials for Privacy (SAOPs) to ensure that appropriate internal privacy protections are in place.

This decentralized and government-only approach is flawed in two ways. Following the 2013 Executive Order on Improving Cybersecurity, each of the SAOPs for the major agencies prepared their assessments of how they were complying with privacy and civil liberties protections in department to department sharing. The detail and level of analysis by the SAOPs differed greatly. Having a decentralized assessment of privacy impacts, including how to intersect with the private sector, will delay the implementation of adequate privacy protections, and will not instill confidence from the private sector. Furthermore, this decentralized approach does not need to take place under the 2015 Executive Order – because DHS has already has an existing infrastructure in place, and it has been identified as the key department in this private sector information-sharing exercise.

It is unfortunate that the 2015 Executive Order did not elaborate on the necessary privacy and civil liberties protections, particularly with regard to private sector information sharing. Nonetheless, the DHS Privacy Office and Office for Civil Rights and Civil Liberties can lead these inter-agency efforts to address private sector concerns, including with the intersection of Information Sharing and Analysis Organizations (ISAOs).

Without a White House-based privacy policy official, the DHS Chief Privacy Officer frequently serves as *de facto* privacy policy leadership between and among the departments and agencies. As I testified before this Subcommittee in April 2013, DHS has taken multiple steps to integrate cybersecurity and privacy as part of the Department's cybersecurity mission. DHS has thoroughly integrated the Fair Information Practice Principles (FIPPs) into its cybersecurity programs. The FIPPS are the "widely accepted framework of defining principles to be used in the evaluation and consideration of systems, processes, or programs that affect individual privacy."[1]

DHS has been quite transparent about its cybersecurity capabilities. As discussed below, transparency is an important tenet under the FIPPs and an important cornerstone to encourage industry participation. DHS has published several Privacy Impact Assessments (PIAs) detailing pilot programs and information sharing among and between government entities as well as with private companies that have signed Cooperative Research and Development Agreements (CRADAs). This work will assist DHS in establishing deeper relationships with new and existing ISAOs.

The Department already has skilled, dedicated privacy professionals who can help navigate the privacy protections needed for effective information sharing, with multiple cyber privacy professionals on staff. These individuals focus on integrating the FIPPs of purpose specification,

[1] The Fair Information Practice Principles as articulated in *National Strategy for Trusted Identities in Cyberspace*, April 2011, available at: http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf

data minimization, use limitation, data quality and integrity and security systematically into all DHS cybersecurity activities.

As part of its mission to implement the FIPPs and to integrate privacy protections into DHS cybersecurity activities, DHS privacy professionals review and provide comments and insight into cybersecurity Standard Operating Procedures (SOPs) (including protocols for human analysis and retention of cyber alerts, signatures, and indicators for minimization of information that could be personally identifiable information), statements of work, contracts, and international cyber-information sharing agreements. The DHS cyber privacy professionals review all of the CRADAs signed with private companies.

An important tenet of the FIPPs is the concept of accountability – periodically reviewing and confirming that the privacy protections initially embedded into any program remain relevant and that those protections are implemented.

While I was DHS Chief Privacy Officer, I instituted "Privacy Compliance Reviews" (PCRs) to confirm the accountability of several of DHS's programs.[2] We designed the PCR to improve a program's ability to comply with assurances made in PIAs, System of Records Notices, and formal information-sharing agreements. The Office conducts PCRs of ongoing DHS programs with program staff to ascertain how required privacy protections are being implemented and to identify areas for improvement.

Given the importance of the DHS mission in cybersecurity, the DHS Privacy Office conducted a Privacy Compliance Review in late 2011, publishing it in early 2012.[3] The DHS Privacy Office found the DHS cybersecurity entities generally complied with the privacy requirements in the relevant Privacy Impact Assessments. Specifically, the DHS cybersecurity entities fully complied with collecting information, using information, internal and external sharing with federal agencies and accountability requirements.

In addition, as this Subcommittee knows, the DHS Chief Privacy Officer has unique investigatory authorities. Therefore, in the unlikely event that something went awry in the future, the Chief Privacy Officer can investigate those activities.[4] This investigatory authority may be of interest to the private companies and ISAOs as more private information starts to flow into the government.

The procedures, staffing, accountability and integration into the relationships with private sector entities through CRADAs demonstrate the way in which privacy protections are integrated throughout the DHS cybersecurity program. A framework is in place to address privacy and civil liberties issues for private sector information sharing, and DHS is well positioned to extend those privacy protections to private sector information sharing on a larger scale.

---

[2] *See DHS Privacy Office Annual Report, July 2011-June 2012* at 39-40 for a detailed discussion of Privacy Compliance Reviews.

[3] *Privacy Compliance Review of the EINSTEIN Program*, January 3, 2012, available at: http://www.dhs.gov/xlibrary/assets/privacy/privacy_privcomrev_nppd_ein.pdf.

[4] 6 U.S.C. § 142(b). *See DHS Privacy Office Annual Report, July 2011-June 2012* at 40 for a discussion of the DHS Chief Privacy Officer investigatory authorities.

Establish Appropriate Limitations on Information Sharing

Consistent with the FIPPs and private sector company expectations, there must be clearly defined controls associated with the cybersecurity threat indicators and the related information.

As the DHS portion of the 2013 Executive Order report noted, there are at least three categories of information that companies may provide when sharing cybersecurity threat indicators – information *directly associated* with the cybersecurity threat, information *related* to the cyber threat, and information *incidentally retained* when sharing the threat indicators themselves.[5]

To limit the amount of incidentally retained and related information being shared, companies should implement strict data minimization standards. Frequently, however, it may not be evident upon initial sharing – especially because time may be of the essence -- which information is directly associated with the cybersecurity threat and which information is either incidentally retained or only related to the cyber threat. Therefore, more information than necessary may be shared. As a result, the federal government/DHS should implement a secondary data minimization review and limit any sharing of information only to the information directly associated with the cyber threat.

In certain discussions, there are recommendations to share all cybersecurity threat information – including the related and incidentally retained information – as soon as possible with all government entities. This is ill-advised, for a few reasons. First, this approach does not assist the other entities in identifying the relevant information and requires each agency to re-analyze the information to determine what is relevant and what is not. That is inefficient. Instead, sharing immediately shifts the burden of implementation and analysis to every entity and decentralizes the skill set. If there is a requirement to immediately share, then more information than necessary – and possibly inaccurate information – will be shared throughout the government. For these two reasons, the experts at DHS should first parse the information and apply data minimization principles to allow other agencies to respond quickly to the threat itself, rather than weeding through potentially disparate layers of information. The same principle of double data minimization applies to information sharing between and among companies.

Widespread sharing of related or incidentally retained information will chill information sharing generally. Companies will not want their non-cyber information shared widely, even if there are use limitations. Providing anonymity for producers (especially private companies) – allowing them an environment to share safely without fear of backlash regarding their vulnerabilities – is vital to encourage cooperation. Companies are legitimately concerned that their valuable trade secrets or business sensitive information may be available to the government and their competitors if the non-cyber threat indicators are not minimized.

Even if cyber threat indicators are judiciously shared, use limitations related to the shared information must be in place. In addition to the liability limitations discussed below, the use of

[5] *Executive Order 13636 Privacy and Civil Liberties Assessment Report 2014*, available at: http://www.dhs.gov/sites/default/files/publications/2014-privacy-and-civil-liberties-assessment-report.pdf

private sector-shared information must be cabined to include only use for cybersecurity threat and response. Relatedly, the federal government (including intelligence agencies) should have limitations on what agencies can retain and for how long with regard to the unique information from companies, rather than the distilled threat indicators.

Civilian Control of the Cybersecurity Information Sharing is Crucial to Encourage Private Information Sharing

Ensuring civilian control of the lifecycle of cybersecurity information from the private sector is critical to comfort private companies before they share cyber threat indicators in volume. Critical infrastructure sectors and companies have reservations that information being shared may not only be used to inform other vulnerable entities, but also would be used for investigations or national security, without any other concomitant benefit. The Executive Order is silent on the issue of civilian control for the lifecycle of the private sector relationship, but that control is crucial to the development of repeatable, consistent information sharing.

Identifying DHS as the private sector interface is vital to placate these concerns. This committee began this process with the legislative establishment of the National Cybersecurity and Communications Integration Center (NCCIC) in 2014 through the National Cybersecurity Protection Act. DHS must continue to be the primary interface with the private sector, and must not just be seen as a pass-through to the intelligence community.

As noted above, DHS has been transparent about its cybersecurity activities, which is imperative to develop credentials and credibility with the private sector. Now that NCCIC has been identified as the leading agency, any information sharing must go through it. As Assistant Secretary Andy Ozment reported to this committee in February, NCCIC received 97,000 incident reports, released 12,000 actionable cyber alerts or warnings and responded to 115 cyber incidents last year. These statistics demonstrate that DHS is maturing. As a civilian agency, it is well positioned to liaise between private companies and the government.

Information Sharing Must Not Threaten Companies

Information sharing must be at an acceptable cost and, therefore, provide minimal risk for the participants. If participants believe they will be targeted by attackers by sharing information, such as configurations, vulnerabilities, or even the fact that they have been targeted, they will not be willing to share information.

DHS has received thorough advice – including from private sector representatives and advocates – as part of its Federal Advisory Committee Act privacy committee, the Data Privacy and Integrity Advisory Committee. The DPIAC issued a significant advisory paper for DHS to consider when implementing information sharing pilots and programs with other entities, including the private sector.[6] The report addresses two important questions in privacy and cybersecurity: "what specific privacy protections should DHS consider when sharing information

[6] *Report from the Cyber Subcommittee to the Data Privacy and Integrity Advisory Committee (DPIAC) on Privacy and Cybersecurity Pilots, Submitted by the DPIAC Cybersecurity Subcommittee,* November 2012, available at: http://www.dhs.gov/sites/default/files/publications/privacy/DPIAC/dpiac_cyberpilots_10_29_2012.pdf.

from a cybersecurity pilot project with other agencies?" and "what privacy considerations should DHS include in evaluating the effectiveness of cybersecurity pilots?" This type of advice helps DHS design systems to avoid antagonizing companies and ISAOs and comfort them they will not somehow be punished for participating.

Limitations on Liability Must Be Clearly Defined

The issue of liability limitations has been discussed at length during the pendency of the cybersecurity legislation. It obviously is an important issue for companies, and it needs to be resolved appropriately in order to encourage information sharing. With that said, having clearly defined limitations may help companies even more than having a "notwithstanding any other law" blanket exception.

The liability limitation must address at least two aspects directly. First, the shared information cannot be shared with other agencies and then used in a civil or criminal enforcement action against the sharing company. That is crucial. Furthermore, the shared information should not be used in civil or criminal enforcement actions against a third party who is not the cyber attacker – namely, if shared information contains damning information either about the sharing company or a third party company, the government's awareness of that information cannot lead to enforcement.

Furthermore, companies and ISAOs need to be comforted that the information they share will be appropriately protected. The DHS transparency on its systems will hopefully ameliorate that concern.

The antitrust concerns raised in earlier Congresses have waned in light of the Joint Department of Justice/Federal Trade Commission Statement *Antitrust Policy Statement on Sharing of Cybersecurity Information*.[7] Nonetheless, more clarity, particularly *vis a vis* inter-company sharing, will induce more information sharing.

Privacy and Civil Liberties Oversight Board Should Be Granted Oversight Authority over Cybersecurity Information Sharing

The Privacy and Civil Liberties Oversight Board (PCLOB) serves an important oversight function on intelligence and national security activities related to terrorism. The PCLOB's authority should be expanded to include oversight on cybersecurity activities, including information sharing with and from the private sector. This addition will further bolster the FIPPs throughout the cyber information sharing lifecycle, and will provide additional oversight capacity over the collection, use, sharing and retention of private sector information.

Thank you for the opportunity to appear before this subcommittee this afternoon. I would be happy to take any questions you may have.

***

[7] http://www.justice.gov/atr/public/guidelines/305027.pdf.