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

STRIKING THE RIGHT BALANCE: PROTECTING OUR NATION'S CRITICAL INFRASTRUCTURE FROM CYBER ATTACK AND ENSURING PRIVACY AND CIVIL LIBERTIES
April 25, 2013 Hearing

Chairman Meehan, Ranking Member Clarke, 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 15 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.

As this Subcommittee knows, the United States' critical infrastructure, including government assets, face significant cybersecurity threats. Cybersecurity and privacy must be integrated in order to most effectively protecting valuable assets. Furthermore, if done right, increased cybersecurity (with appropriate standards and procedures) also means increased privacy.

The Department of Homeland Security has taken multiple steps to integrate cybersecurity and privacy as part of the Department's cybersecurity mission. In fact, DHS has integrated privacy into its cybersecurity program since the EINSTEIN program was launched in late 2003. Shortly thereafter, the Department published one of the its first Privacy Impact Assessments (PIA) on EINSTEIN 1 (a network flow system), detailing the privacy protections that DHS embedded into its cybersecurity program from the beginning, and being transparent about those protections.[1] In 2008, DHS conducted a PIA on the second iteration of the DHS cybersecurity program, EINSTEIN 2 (adding an intrusion detection capability).[2] These PIAs exemplify the concept of "privacy by design" and are important foundational considerations for a large operational department like DHS.

[1] EINSTEIN 1, developed in 2003, provides an automated process for collecting computer network security information from voluntary participating federal executive agencies. It works by analyzing network flow records. Even though DHS was not required to do a PIA given no personally identifiable information (PII) was being collected, DHS conducted a PIA (DHS/NPPD/PIA/001) on EINSTEIN 1 in September 2004 for transparency, available at: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_eisntein.pdf.

[2] As with EINSTEIN 1, EINSTEIN 2 passively observes network traffic to and from participating federal Executive Branch departments and agencies' networks. In addition, EINSTEIN 2 adds an intrusion detection system capability that alerts when a pre-defined specific cyber threat is detected and provides the US-CERT with increased insight into the nature of that activity. The May 2008 PIA (DHS/NPPD/PIA-008) is available at: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_einstein2.pdf.

I. DHS INTEGRATION OF PRIVACY PROTECTIONS INTO ITS CYBERSECURITY PROGRAMS

During my three and a half year tenure at DHS, we further integrated privacy into the DHS cybersecurity programs in several ways.

1. **Integration of the Fair Information Practice Principles into DHS Cybersecurity Programs**: As noted below, 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."[3]

   The FIPPs are eight interdependent principles that create a framework for how information may be used and shared in a manner that protects privacy: transparency; individual participation; purpose specification; data minimization; use limitation; data quality and integrity; security; and accountability and auditing.[4] During my tenure, my office worked tirelessly to integrate the FIPPs into all DHS programs, including cybersecurity.

2. **Transparency**: DHS has been very transparent about its cybersecurity capabilities. During my tenure, DHS published several PIAs detailing pilot programs and information sharing among and between different government entities. First, DHS discussed via PIA a 12-month proof of concept to determine the benefits and issues presented by deploying the EINSTEIN 1 capability to Michigan state government networks managed by the Michigan Department of Information Technology.[5] Shortly thereafter, DHS completed both a classified and unclassified PIA for the "Initiative Three Exercise"[6] of the Comprehensive National Cybersecurity Initiative."[7] In the Initiative Three Exercise, DHS engaged in an exercise to demonstrate a suite of technologies that could be included in the next generation of the Department's EINSTEIN network security program, such as an intrusion prevention capability. This demonstration used a modified complement of system components then being provided by the EINSTEIN 1 and EINSTEIN 2 capabilities, as well as a DHS test deployment of technology developed by the National Security Agency (NSA) that included an intrusion prevention capability. The DHS Privacy Office worked with DHS and the NSA to be as transparent as possible with the Exercise, including naming NSA (and its role in the Exercise) expressly in the PIA.

---

[3] *National Strategy for Trusted Identities in Cyberspace*, April 2011, available at: http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf

[4] DHS adopted the eight FIPPs as a framework for Privacy Policy on December 29, 2008; see *DHS Privacy Policy Guidance Memorandum 2008-01*, available at: http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

[5] *Privacy Impact Assessment Update for the EINSTEIN 1: Michigan Proof of Concept*, February 19, 2010, (DHS/NPPD/PIA-013) available at: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_nppd_einstein1michigan.pdf.

[6] *US-CERT: Initiative Three Exercise Privacy Impact Assessment (unclassified)*, March 18, 2010, (DHS/NPPD/PIA-014) available at: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_nppd_initiative3.pdf.

[7] *See* http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative for a description of all 12 cybersecurity initiatives.

In early 2012, DHS published a PIA on its information sharing pilot with the Defense Industrial Base;[8] after 180 days and a series of evaluations of its effectiveness, the PIA was updated to reflect the establishment of a permanent program to enhance cybersecurity of participating Defense Industrial Base entities through information sharing partnerships. The permanent program was announced via PIA shortly before my departure.[9]

Furthermore, one of my last acts as Chief Privacy Officer was to approve a comprehensive PIA that described the entire National Cybersecurity Protection System (NCPS), a programmatic PIA that explains and integrates all the NPPD/Cybersecurity and Communication (CS&C) cyber programs in a holistic document, rather than the previous patchwork PIAs that were snapshots in time of CS&C capabilities.[10] This NCPS PIA helps provide a comprehensive understanding of the CS&C cybersecurity program, further increasing transparency.

3. **Outreach and engagement with advocates and private sector representatives:** The Department engaged privacy and civil liberties advocates and private sector representatives about its cybersecurity activities in several ways. First, as part of the *Cyberspace Policy Review* conducted by the Administration in 2009,[11] the Department met with privacy and civil liberties advocates and academicians (at a Top Secret/SCI level) to discuss the Advanced Persistent Threat landscape, and government response. That ad hoc meeting led to the creation of a subcommittee of DHS' Federal Advisory Committee Act-authorized committee, the Data Privacy and Integrity Advisory Committee (DPIAC).[12] The members and the experts on the DPIAC subcommittee (including privacy and civil liberties advocates, academicians, and private sector representatives) were briefed frequently at the Top Secret/SCI level. After my departure, the DPIAC subcommittee produced an excellent report on integrating privacy into the DHS information sharing pilots and programs, discussed below.

---

[8] *Privacy Impact Assessment for the National Cyber Security Division Joint Cybersecurity Services Pilot (JCSP)*, January 16, 2012, (DHS/NPPD/PIA-021) available at: http://www.dhs.gov/xlibrary/assets/privacy/privacy_nppd_jcsp_pia.pdf. (*N.B.*, this PIA has been retired with the release of the ECS PIA in January 2013, referenced below).

[9] *Privacy Impact Assessment Update for the Joint Cybersecurity Services Program (JCSP), Defense Industrial Base (DIB) – Enhanced Cybersecurity Services (DECS)*, July 18, 2012, (DHS/NPPD/PIA-021(a)) available at: http://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-update-nppd-jcps.pdf. (*N.B.*, this PIA update has been retired with the release of the ECS PIA in January 2013, referenced below).

[10] *National Cybersecurity Protection Program Privacy Impact Assessment*, July 30, 2012,(DHS/NPPD/PIA-026) available at: http://www.dhs.gov/sites/default/files/publications/privacy/privacy-pia-nppd-ncps.pdf.

[11] *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, 2009, available at: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

[12] The DHS Data Privacy and Integrity Advisory Committee provides advice at the request of the Secretary of Homeland Security and the DHS Chief Privacy Officer on programmatic, policy, operational, administrative, and technological issues within the DHS that relate to PII, as well as data integrity and other privacy-related matters. The committee was established by the Secretary of Homeland Security under the authority of 6 U.S.C. § 451 and operates in accordance with the provisions of the Federal Advisory Committee Act (FACA) (5 U.S.C. App).

In addition to the systematic engagement of advocates, academicians, and private sector representatives through the DPIAC subcommittee, DHS also discussed its embedded privacy and cybersecurity protections in several public fora, including Congressional testimony,[13] public articles,[14] and multiple public presentations before the DPIAC on DHS cyber activities.[15]

The DHS Privacy Office (and NPPD) also frequently met with privacy advocates to discuss cybersecurity considerations, either when a new program or initiative was announced, or during the quarterly Privacy Information for Advocates meetings instituted in 2009.[16]

4. **Dedicated Cyber Privacy Personnel**: To be engaged and be able to effectively integrate privacy protections, the Department has hired multiple cyber privacy professionals. These cyber privacy professionals focus on integrating the FIPPs of purpose specification, data minimization, use limitation, data quality and integrity, and security systematically into NCSD activities. For example, the Senior Privacy Officer for the National Protection and Program Directorate (reporting to the Directorate leadership) was hired in August 2010; she has a dedicated privacy analyst on-site with CS&C and both are integrated into planning and implementation processes. In the DHS Privacy Office, there has been a liaison with NPPD cybersecurity organizations since the first EINSTEIN PIA was written; currently that position is Director, Privacy and Technology. This Director of Privacy and Technology was, for a period of time, embedded at the NSA as part of the development of the enhanced relationship between the NSA and DHS.[17]

---

[13] *See, e.g., The Cybersecurity Partnership Between the Private Sector and Our Government: Protecting Our National and Economic Security*, Joint Committee Hearing before Senate Committee on Homeland Security and Governmental Affairs and Senate Committee on Commerce, Science, and Transportation, March 7, 2013 (testimony of Secretary Janet Napolitano); *DHS Cybersecurity: Roles and Responsibilities to Protect the Nation's Critical Infrastructure*, Hearing before House Committee on Homeland Security, March 13, 2013 (testimony of Deputy Secretary Jane Holl Lute); *Examining the Cyber Threat to Critical Infrastructure and the American Economy*, Hearing before House Committee on Homeland Security, March 16, 2011 (testimony of NPPD Deputy Undersecretary Philip Reitinger).

[14] *See, e.g., Securing Cyberspace while Protecting Privacy and Civil Liberties*, Homeland Security Blog (by Secretary Janet Napolitano), April 2, 2013, available at: http://www.dhs.gov/blog/2013/04/02/securing-cyberspace-while-protecting-privacy-and-civil-liberties; *Op-Ed: A Civil Perspective on Cybersecurity*, (Jane Holl Lute and Bruce McConnell), WIRED, February 14, 2011, available at: http://www.wired.com/threatlevel/2011/02/dhs-op-ed/all/.

[15] *See, e.g.*, on March 18, 2010, Deputy Assistant Secretary for Cybersecurity and Communications Michael A. Brown presented to DPIAC on computer network security and related privacy protections in DHS, including the Department's role in the CNCI (focusing on the DHS Privacy Office's work on PIAs for EINSTEIN 1, EINSTEIN 2, and the proof of concept pilot project of the EINSTEIN 1 capabilities with the U.S. Computer Readiness Team and the State of Michigan), the National Cyber Incident Response Plan (NCIRP), and the National Cybersecurity and Communications Integration Center, US-CERT, DHS I&A, and the National Cybersecurity Center; on July 11, 2011, the Senior Privacy Officer for NPPD Emily Andrew described how her office was integrated into the NPPD structure.

[16] *See DHS Privacy Office Annual Report, July 2009 to June 2010* at 66 for a discussion of the Privacy Information for Advocates quarterly meetings, available at: http://www.dhs.gov/xlibrary/assets/privacy/privacy_rpt_annual_2010.pdf.

[17] *Memorandum of Agreement Between The Department of Homeland Security and The Department of Defense Regarding Cybersecurity*, September 2010, available at: http://www.dhs.gov/xlibrary/assets/20101013-dod-dhs-cyber-moa.pdf.

When I was Chief Privacy Officer, I actively participated in numerous cybersecurity policy planning organizations within the Department.

5. **Involvement and Coordination on Standard Operating Procedures, and Operational Aspects of 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 PII), statements of work, contracts, and international cyber-information sharing agreements.

6. **Cyber-specific Privacy Training for Cybersecurity Analysts and Federal Privacy Professionals**: These cyber privacy professionals provide cyber-specific privacy training to cybersecurity analysts to supplement the privacy training required for DHS employees and contractors. In my opinion as a privacy professional, the more relevant and concrete you can make privacy training, the more likely the audience will understand and incorporate privacy protections into their daily activities, thus increasing personal accountability.

   During my tenure, the Department also engaged in a year-long Speakers Series for members of the federal government community to discuss privacy and cybersecurity issues, and their impact on federal operations.[18] The federal government-wide access to the Speakers Series helped enhance awareness of the cybersecurity and privacy issues, along with providing an interagency communications channel on privacy and cybersecurity questions.

7. **Accountability of the Cybersecurity Program through Privacy Compliance Review:** 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.[19] 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.

[18] *See DHS Privacy Office Annual Report, July 2011-June 2012* at 27 for a discussion of the four-part Speakers Series, available at: http://www.dhs.gov/sites/default/files/publications/privacy/Reports/dhs_privacyoffice_2012annualreport_September2012.pdf.

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

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.[20] The DHS Privacy Office found NPPD/CS&C generally compliant with the requirements outlined in the EINSTEIN 2 PIA and Initiative 3 Exercise PIA. Specifically, NPPD/CS&C was fully compliant on collection of information, use of information, internal sharing and external sharing with federal agencies, and accountability requirements.

My office made five recommendations to strengthen program oversight, external sharing, and bring NPPD/CS&C into full compliance with data retention and training requirements. NPPD agreed with our findings and, as I understand it, has taken multiple steps to address our recommendations. For example, in response to one of the recommendations, the NPPD Office of Privacy now conducts quarterly reviews of signatures and handling of personally identifiable information. These reviews have provided increased awareness to US-CERT Staff and has helped to build positive working relationships with cyber analysts and leadership. This is important in continuing to integrate cybersecurity and privacy, by understanding the impact of each.

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.[21]

II. DHS CONTINUES TO INTEGRATE PRIVACY PROTECTIONS INTO ITS CYBERSECURITY PROGRAMS

Since I left DHS, I know through public information that the Department continues to work to embed privacy protections in its cybersecurity activities.

A. DPIAC Cybersecurity Report

The DPIAC issued a robust advisory paper for DHS to consider when implementing information sharing pilots and programs with other entities, including the private sector.[22] The report addresses two important questions in privacy and cybersecurity -- "what specific privacy protections should DHS consider when sharing information from a cybersecurity pilot project with other agencies?" and "what privacy considerations should DHS include in evaluating the effectiveness of cybersecurity pilots?"

The DPIAC report supported in large part what DHS had been doing with regard to privacy protections incorporated in its cybersecurity pilots and programs. DPIAC recommended the following best practices when sharing information from a cybersecurity pilot project with other

[20] *Privacy Compliance Review of the EINSTEIN Program*, January 3, 2012, available at: http://www.dhs.gov/xlibrary/assets/privacy/privacy_privcomrev_nppd_ein.pdf.
[21] 6 U.S.C. § 142(b). *See ibid., DHS Privacy Office Annual Report, July 2011-June 2012* at 40 for a discussion of the DHS Chief Privacy Officer investigatory authorities.
[22] *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.

agencies: incorporate the FIPPs into cybersecurity activities; develop and implement clear data minimization rules and policies; provide employees and public users of federal systems notice and transparency of the collection, use, and sharing of information for cybersecurity purposes; when engaging in information sharing that includes PII or content of private communications, information sharing should be limited to what is necessary to serve the pilot's purposes (with defined limits on law enforcement, national security, and civilian agency sharing); have more robust safeguards for information from private networks; define data retention policies to keep records no longer than needed to fulfill the purpose of the pilot; and integrate privacy by design and privacy enhancing technologies whenever possible.

This type of insight from privacy advocates, academicians, and private sector representatives will enhance DHS' considerations of privacy-protective options when sharing cybersecurity information.

B. Enhanced Cybersecurity Services PIA

Furthermore, in January 2013, DHS published a thoughtful and comprehensive PIA covering the Enhanced Cybersecurity Services (ECS), a voluntary program based on the sharing of indicators of malicious cyber activity between DHS and participating Commercial Service Providers.[23] The purpose of the program is to assist the owners and operators of critical infrastructure to enhance the protection of their systems from unauthorized access, exploitation, or data exfiltration through a voluntary information sharing program. ECS is intended to support U.S. critical infrastructure, however, pending deployment of EINSTEIN intrusion prevention capabilities, ECS may also be used to provide equivalent protection to participating federal civilian Executive Branch agencies.[24]

The ECS PIA is exemplary of how to integrate privacy protections into cybersecurity programs, particularly when engaging in information sharing with the private sector. This ECS PIA is the culmination of all of the hard work that I summarized above, including the DPIAC cybersecurity report.

It is clear DHS continues to embed privacy protections into cybersecurity activities. The information sharing and implementation standards described in the ECS PIA are concrete examples of privacy by design, and should well position DHS to effectively implement the increased information sharing mandated by the February 12, 2013 *Executive Order on Improving Critical Infrastructure Cybersecurity*.[25]

---

[23] *Privacy Impact Assessment for the Enhanced Cybersecurity Services (ECS)*, January 16, 2013, DHS/NPPD/PIA-028, available at: http://www.dhs.gov/sites/default/files/publications/privacy/privacy_pia_nppd_ecs_jan2013.pdf.

[24] This PIA consolidates and serves as a replacement to the two PIAs I mentioned earlier: DHS/NPPD/PIA-021 *National Cyber Security Division Joint Cybersecurity Services Pilot PIA*, published on January 13, 2012, and the DHS/NPPD/PIA-021(a) *National Cyber Security Division Joint Cybersecurity Services Program (JCSP), Defense Industrial Base (DIB) – Enhanced Cybersecurity Services (DECS)* PIA Update, published on July 18, 2012.

[25] *Executive Order on Improving Critical Infrastructure Cybersecurity*, available at: http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

C. EINSTEIN 3 Accelerated (E^3A) PIA

In addition, just this week, the Department announced that it will deploy EINSTEIN 3 Accelerated (E^3A) network intrusion prevention capabilities on federal government networks as a Managed Security Service provided by Internet Service Providers (ISPs), rather than placing the entire response on the federal government.[26]

The use of ISPs as a Managed Security Service is noteworthy from a privacy perspective for several reasons. First, the coordination and collaboration of the "best of breed" federal classified and unclassified capabilities combined with the nimbleness (and proprietary capabilities) of the private sector ISPs will allow a more robust response to evolving cybersecurity threats. It is an important recognition by DHS that federal cybersecurity programs did not need to re-invent cybersecurity protections when defending federal government networks, but could supplement existing commercial intrusion prevention security systems to provide a more robust prevention and detection regime for the federal civilian Executive Branch.

Second, integrating cybersecurity threat detection and intrusion prevention will allow DHS to better detect, respond to, or appropriately counter, known or suspected cyber threats within the federal network traffic it monitors, which helps protect the target systems from unauthorized intrusions (and therefore implements the security FIPP). It is important to emphasize – E^3A monitors only select Internet traffic either destined to, or originating from, federal civilian Executive Branch departments and agencies (commonly known as .gov traffic). This data minimization and segregation is also privacy-protective; the ISP Managed Security Service can be compartmentalized to affect only .gov traffic. The participating agencies will identify a list of IP addresses for their networks and both CS&C cybersecurity analysts and the ISPs verify the accuracy of the list of IP addresses provided by the agency. CS&C SOPs are followed in the event of any out-of-range network traffic is identified and the ISP removes any collected data to prevent any further collection of this network traffic. This too is a privacy-protective approach, further confirming that the only impacted traffic is federal civilian Executive Branch departments and agencies.

DHS will share cyber threat information it receives through E^3A consistent with its existing policies and procedures (which have been thoroughly reviewed by the Department's cyber privacy professionals). In accordance with the SOPs and information handling guidelines, all information that could be considered PII is reviewed prior to inclusion in any analytical product or other form of dissemination, and replaced with a generic label when possible, again protecting privacy. The way E^3A is structured should enhance privacy, protect the federal civilian Executive Branch departments and agencies, and provide a nimble response to the evolving cybersecurity threat.

---

[26] *Privacy Impact Assessment for EINSTEIN 3 -Accelerated (*E^3A*),* April 19, 2013 (DHS/PIA/NPPD-027), available at: http://www.dhs.gov/sites/default/files/publications/privacy/PIAs/PIA%20NPPD%20E3A%2020130419%20FINAL%20signed.pdf.

III. INTEGRATION OF PRIVACY PRINCIPLES INTO CYBERSECURITY IS CRUCIAL FOR EFFECTIVE CYBERSECURITY PROGRAMS

The continued integration of privacy and cybersecurity is crucial for effective cybersecurity protections. In my experience based on 15 years as a privacy professional as both outside counsel and Chief Privacy Officer at DHS, it is clear that integrating privacy into the operational aspects of any activity makes the program both more effective and more likely to protect privacy. For example, providing tailored training, and engaging the analysts or employees in the field facilitates the integration of privacy into daily operations. *Ex ante* review of programs and anticipating issues such as unintended uses, data minimization, and defined standards for information sharing are also important to confirm privacy protections are working throughout the lifecycle of information collection. Embedding privacy protections into SOPs and information handling guidelines help to further the goal of the project while assuring that privacy protections are systematically integrated into a program or service. Finally, transparency is the cornerstone for any privacy program to succeed.

These privacy-by-design factors are important any time an organization incorporates privacy into a new program, but they are particularly important with an operational cybersecurity program such the DHS National Cybersecurity Protection System which continuously counters emerging cybersecurity threats and applies effective risk mitigation strategies to detect and deter these threats. Integrating privacy from the beginning – and periodically testing to confirm that the integration continues – is the only way to effectively protect cybersecurity *and* privacy. In fact, if done right, increased cybersecurity also means increased privacy.

To address threats and minimize the impact on federal facilities and critical infrastructure, key agencies and critical infrastructure companies must share information about cybersecurity threats. That said, such information sharing must occur in a thoughtful, clearly-designed process that also minimizes the impact on individual privacy. I believe that DHS has appropriately and effectively integrated privacy and cybersecurity both in its federal Executive Branch responsibilities and in its information-sharing responsibilities as articulated in the ECS and related cybersecurity PIAs. Currently, I advise private sector clients that this privacy-by-design approach should be taken to most effectively combat cybersecurity threats by both increasing cybersecurity protections and protecting privacy.

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

***