Executive Order 13636

Privacy and Civil Liberties Assessment Report

Compiled by

The Privacy Office and the Office for Civil Rights and Civil Liberties

Department of Homeland Security

April 2014

FOREWORD

April 2014

We are pleased to present the 2014 Executive Order 13636 Privacy and Civil Liberties Assessments Report. On February 12, 2013, President Obama issued Executive Order 13636, *Improving Critical Infrastructure Cybersecurity* (EO) and Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience* (PPD-21), directing federal departments and agencies to work together and with the private sector to strengthen the security and resilience of the Nation's critical infrastructure. The EO requires federal agencies to develop and incentivize participation in a technology-neutral cybersecurity framework, to increase the volume, timeliness, and quality of cyber threat information it shares with the private sector, and to work with their senior agency officials for privacy and civil liberties to ensure that privacy and civil liberties protections are incorporated into all of these activities.

Section 5 of the EO also requires that senior agency officials for privacy and civil liberties assess the privacy and civil liberties impacts of the activities their respective departments and agencies have undertaken pursuant to the EO, and to publish their assessments annually in a report compiled by our offices. This is the first such annual report. It includes our offices' assessments of certain DHS activities under Section 4 of the EO (enhanced threat information sharing with the private sector) as well as assessments conducted independently by the Department of the Treasury and the Departments of Defense, Justice, Commerce, Health and Human Services, Transportation, and Energy, and by the Office of the Director of National Intelligence and the General Services Administration.

As the programs and activities called for in the EO mature and evolve, departments and agencies, including DHS, will conduct additional assessments as needed and include them in future annual reports.

Megan H. Mack
Officer for Civil Rights and Civil Liberties

Karen L. Neuman
Chief Privacy Officer

INTRODUCTION

Background

On February 12, 2013, President Obama issued Executive Order 13636, *Improving Critical Infrastructure Cybersecurity* (EO), and Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience* (PPD-21), directing federal departments and agencies to work together and with the private sector to strengthen the security and resilience of the Nation's critical infrastructure (CI) against evolving threats and hazards.[1] The EO and PPD-21 call for an updated and overarching national framework that reflects the increasing role of cybersecurity in securing physical CI. The EO directs federal departments and agencies to:

- Develop a technology-neutral voluntary cybersecurity framework;
- Promote and incentivize the adoption of cybersecurity practices;
- Increase the volume, timeliness, and quality of cyber threat information sharing;
- Explore the use of existing regulation to promote cyber security; and
- Incorporate strong privacy and civil liberties protections into every initiative to secure our CI.

PPD-21 directs federal departments and agencies to:

- Develop a situational awareness capability that addresses both physical and cyber aspects of how infrastructure is functioning in near-real time;
- Understand the cascading consequences of infrastructure failures;
- Evaluate and mature the public-private partnership;
- Update the National Infrastructure Protection Plan to take into account cyber aspects of infrastructure; and
- Develop a comprehensive research and development plan.

The EO and PPD-21 designated the Department of Homeland Security (DHS) as the lead for federal efforts to implement these requirements. To that end, DHS established an Integrated Task Force (ITF) to coordinate interagency and public and private sector efforts, and to ensure effective integration and synchronization of implementation across the homeland security enterprise. The ITF included several Working Groups, each focused on specific deliverables of implementation, and was led by a Director and Deputy Director whose work was governed by an Executive Steering Committee, which reported to the DHS Deputy Secretary. The ITF worked for 10 months to achieve the implementation timeline directed by the EO and PPD-21 before turning the EO and PPD work back to the DHS program offices and Sector Specific Agencies (SSA) responsible for ongoing execution of the required deliverables. Throughout its work, the

[1] Links to both the EO and PPD-21 are available on the Department of Homeland Security's website at http://www.dhs.gov/strengthening-security-and-resilience-nation%E2%80%99s-critical-infrastructure.

ITF and its Working Groups engaged in an unprecedented outreach effort to ensure that the deliverables required by the EO and PPD-21 were informed by the views and input of the full range of public and private sector stakeholders.[2]

The 2014 EO 13636 Privacy and Civil Liberties Assessments Report

Responsibility to Protect Privacy and Civil Liberties

Section 5 of the EO provides that:

> *[a]gencies shall coordinate their activities under this order with their senior agency officials for privacy and civil liberties and ensure that privacy and civil liberties protections are incorporated into such activities. Such protections shall be based upon the Fair Information Practice Principles and other privacy and civil liberties policies, principles, and frameworks as they apply to each agency's activities*.

Thus, privacy and civil liberties protections are central to agency activities undertaken pursuant to the EO.

Reporting Requirements

Section 5 also requires the DHS Chief Privacy Officer and Officer for Civil Rights and Civil Liberties to assess the privacy and civil liberties impacts of the activities DHS undertakes pursuant to the EO and to provide those assessments, together with recommendations for mitigating identified privacy risks, in an annual public report.[3] The EO requires senior agency officials for privacy and civil liberties in other federal departments and agencies to conduct assessments of their respective activities and provide those assessments to DHS for inclusion in the annual report.[4]

Report Structure and Content

This report is the first annual report under Section 5 of the EO. It includes the DHS Privacy Office's and Office for Civil Rights and Civil Liberties' (CRCL) assessments of DHS activities undertaken pursuant to Section 4 of the EO. This report also includes submissions from the following departments and agencies:

- The Department of the Treasury
- The Department of Defense
- The Department of Justice
- The Department of Commerce

[2] The Consultative Process developed by the ITF under Section 6 of the EO will continue to ensure stakeholder involvement in the ongoing work to provide cybersecurity for CI. A complete description of the Consultative Process and detailed information on the deliverables accomplished under the EO and PPD-21 are available at www.dhs.gov/eoppd.
[3] EO Section 5(b).
[4] EO Section 5(b). The EO provides for a classified annex to the report as needed.

- The Department of Health and Human Services
- The Department of Transportation
- The Department of Energy
- The Office of the Director of National Intelligence
- The General Services Administration

Staff of the DHS Privacy Office and CRCL co-chaired the ITF's Assessments Working Group, whose members included privacy and civil liberties officials from departments and agencies throughout the Federal Government. Unlike the other ITF Working Groups, the Assessments Working Group did not have an assigned deliverable, but instead served as a forum for participating federal departments and agencies to discuss best practices in conducting privacy and civil liberties assessments generally, to further work on their respective assessments.

As Section 5 of the EO requires, DHS has served as the compiling agency for this report. The privacy and civil liberties officials of the participating departments and agencies conducted their assessments independently when, in their professional judgment, it was appropriate to do so. Their contributions appear below in separate sections for each submitting department or agency. It should be recognized that not all departments and agencies used the same reporting period for their assessments, as progress on deliverables was fluid and department and agency clearance procedures differ. As the programs and activities called for in the EO mature and evolve, departments and agencies, including DHS, will conduct additional assessments as needed and include them in future annual reports.

Table of Submissions

PART I

DEPARTMENT OF HOMELAND SECURITY

Department of Homeland Security
EO 13636 Assessments
Table of Contents

I. Introduction

The DHS Privacy Office

The Privacy Office is the first statutorily created privacy office in any federal agency, as set forth in Section 222 of the *Homeland Security Act* (Homeland Security Act), as amended.[5] The mission of the Privacy Office is to protect all individuals by embedding and enforcing privacy protections and transparency in all DHS activities. The Privacy Office works to minimize the impact of DHS programs on an individual's privacy, particularly an individual's personal information, while achieving the Department's mission to protect the homeland. The Chief Privacy Officer reports directly to the Secretary of Homeland Security.

The DHS Privacy Office accomplishes its mission by focusing on the following core activities:

- Requiring compliance with federal privacy and disclosure laws and policies in all DHS programs, systems, and operations, including cybersecurity-related activities;
- Centralizing Freedom of Information Act (FOIA) and Privacy Act operations to provide policy and programmatic oversight, to support operational implementation within the DHS components, and to ensure the consistent handling of disclosure requests;
- Providing leadership and guidance to promote a culture of privacy and adherence to the Fair Information Practice Principles across the Department;
- Advancing privacy protections throughout the Federal Government through active participation in interagency fora;
- Conducting outreach to the Department's international partners to promote understanding of the U.S. privacy framework generally and the Department's role in protecting individual privacy; and,
- Ensuring transparency to the public through published materials, reports, formal notices, public workshops, and meetings.[6]

The DHS Office for Civil Rights and Civil Liberties

The Department of Homeland Security Office for Civil Rights and Civil Liberties (CRCL) supports the Department's mission to secure the nation while preserving individual liberty, fairness, and equality under the law. The Office for Civil Rights and Civil Liberties reports directly to the Secretary of Homeland Security. CRCL integrates civil rights and civil liberties into all of the Department activities by:

[5] 6 U.S.C. § 142.

[6] Detailed information about DHS Privacy Office activities and responsibilities, including Privacy Impact Assessments conducted by the Privacy Office for DHS cybersecurity-related efforts, is available at http://www.dhs.gov/privacy.

- Promoting respect for civil rights and civil liberties in policy creation and implementation by advising Department leadership and personnel;
- Communicating with individuals and communities whose civil rights and civil liberties may be affected by Department activities, informing them about policies and avenues of redress, and promoting appropriate attention within the Department to their experiences and concerns;
- Investigating and resolving civil rights and civil liberties complaints filed by the public regarding Department policies or activities, or actions taken by Department personnel; and
- Leading the Department's equal employment opportunity programs and promoting workforce diversity and merit system principles.[7]

DHS Methodology for Conducting Executive Order (EO) 13636 Assessments

The DHS Privacy Framework

The Fair Information Practice Principles (FIPPs), which are rooted in the tenets of the Privacy Act of 1974,[8] have served as DHS's core privacy framework since the Department was established. They are memorialized in the DHS Privacy Office's *Privacy Policy Guidance Memorandum 2008-01, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security*[9] and in DHS Directive 047-01, *Privacy Policy and Compliance* (July 2011).[10] The DHS implementation of the FIPPs is as follows:

> **Transparency:** DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of Personally Identifiable Information (PII). Technologies or systems using PII must be described in a SORN and PIA, as appropriate. There should be no system the existence of which is a secret.
>
> **Individual Participation:** DHS should involve the individual in the process of using PII. DHS should, to the extent practical, seek individual consent for the collection, use, dissemination, and maintenance of PII and should provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.
>
> **Purpose Specification:** DHS should specifically articulate the authority which permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.

[7] Detailed information about the activities and responsibilities of the DHS CRCL is available at http://www.dhs.gov/office-civil-rights-and-civil-liberties.
[8] 5 U.S.C. § 552a.
[9] Available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.
[10] Directive 047-01 is available at http://www.dhs.gov/xlibrary/assets/foia/privacy-policy-compliance-directive-047-01.pdf. The Directive supersedes the DHS Directive 0470.2, *Privacy Act Compliance*, which was issued in October 2005.

Data Minimization: DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s). PII should be disposed of in accordance with DHS records disposition schedules as approved by the National Archives and Records Administration.

Use Limitation: DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.

Data Quality and Integrity: DHS should, to the extent practical, ensure that PII is accurate, relevant, timely, and complete, within the context of each use of the PII.

Security: DHS should protect PII (in all forms) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

Accountability and Auditing: DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

The FIPPs govern the appropriate use of PII at the Department. DHS uses the FIPPs to enhance privacy protections by assessing the nature and purpose of all PII collected to ensure it fulfills the Department's mission to preserve, protect, and secure the homeland. The DHS Privacy Office applies the FIPPs to the full breadth and diversity of Department systems, programs, and initiatives that use PII or are otherwise privacy-sensitive, including the Department's cybersecurity-related activities. The Privacy Office works with Department personnel to complete Privacy Threshold Analyses (PTA),[11] Privacy Impact Assessments (PIA),[12] and System of Records Notices (SORN)[13] to ensure implementation of privacy policy at DHS, to

[11] The first step in the DHS privacy compliance process is for DHS staff seeking to implement or modify a system, program, technology, or rulemaking to complete a PTA. The Privacy Office reviews and adjudicates the PTA, which serves as the official determination as to whether or not the system, program, technology, or rulemaking is privacy sensitive and requires additional privacy compliance documentation such as a PIA or SORN.

[12] The E-Government Act and the Homeland Security Act require PIAs, and PIAs may also be required in accordance with DHS policy issued pursuant to the Chief Privacy Officer's statutory authority. PIAs are an important tool for examining the privacy impact of IT systems, initiatives, programs, technologies, or rulemakings. The DHS PIA is based on the FIPPs framework and covers areas such as the scope and use of information collected, information security, and information sharing. Each section of the PIA concludes with analysis designed to outline any potential privacy risks identified in the answers to the preceding questions and to discuss any strategies or practices used to mitigate those risks. The analysis section reinforces critical thinking about ways to enhance the natural course of system development by including privacy in the early stages. PIAs are initially developed in the DHS Components, with input from the DHS Privacy Office. Once approved at the Component level, PIAs are submitted to the DHS Chief Privacy Officer for final approval. Once approved, PIAs are published on the Privacy Office website, with the exception of a small number of PIAs for national security systems.

[13] The Privacy Act requires that federal agencies issue a SORN to provide the public notice regarding PII collected in a system of records. A system of records means a group of records under the control of the agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. SORNs explain how the information is used, retained, and may be corrected, and whether certain portions of the system are subject to Privacy Act exemptions for law enforcement or national security reasons. If a SORN is required, the program manager will work with the Component Privacy Officer or

demonstrate accountability, and to further the transparency of Department activities. PIAs and SORNs relevant to the Department's activities under EO Section 4 are discussed in the assessments reported below.

Civil Rights and Civil Liberties Assessment Framework

CRCL conducts assessments using an issue-spotting approach rather than a single framework because the particular issues presented by any given program or activity vary greatly. The generalized approach is to do an in-depth factual examination of a program or activity to determine how it is intended to work and how it does, or will work in practice. Next, CRCL considers relevant legal and policy authorities to ensure compliance, then evaluates whether a program or activity should be modified to improve the protection of individual rights. The standards applied to evaluate programs and activities include:

- Individual rights and constraints on government action provided for in the Constitution of the United States.
- Statutory protections of individual rights, such as the Civil Rights Act of 1964, 42 U.S.C. §§ 1981-2000h-6.
- Statutes that indirectly serve to protect individuals, such as the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-2522.
- Executive Orders, Regulations, Policies, and other rules or guidelines that direct government action and define the government's relationship to the individual in specific circumstances.
- Other sources of law or authority that may be relevant in specific instances, such as international law standards pertaining to human rights, or prudential guidelines suggesting best practices for governance of particular types of government activities.

The assessment process typically results in the evaluation of several possible individual rights questions raised by a program or activity. The most salient of the factual findings and legal and policy concerns are then addressed in policy advice and within a civil liberties impact assessment or comparable document. CRCL then works with the DHS elements involved to craft workable policy recommendations and solutions to ensure individual rights are appropriately protected within the assessed program or activity.

Related DHS Privacy and Civil Liberties Activities

In addition to leading the Integrated Task Force's (ITF) Assessments Working Group, the DHS Privacy Office and CRCL have been actively involved in implementing the EO within DHS. They actively participated in the ITF Working Groups whose deliverables could impact privacy and civil liberties to ensure that appropriate protections were included. To provide transparency

---

Privacy Point of Contact and Component counsel to write the SORN for submission to the Privacy Office. The DHS Chief Privacy Officer reviews, signs, and publishes all DHS SORNs.

into the Department's and the ITF's work related to the EO, and to provide an opportunity for public input into the implementation process, the Offices hosted a series of five bi-weekly public meetings in April and May 2013, bringing the advocates together with ITF leadership.

These efforts were a continuation of Department efforts to provide transparency into its National Protection and Programs Directorate's (NPPD) cybersecurity-related activities dating back to PIAs and SORNs published in 2004.[14] In addition, the Department has sought the guidance of its Data Privacy and Integrity Advisory Committee (DPIAC)[15] on cybersecurity-related matters. The DHS Privacy Office has briefed the Committee on cybersecurity-related matters in numerous public meetings. At the Chief Privacy Officer's request, the DPIAC issued a public report and recommendations on implementing privacy in cybersecurity pilot programs. The report, which was issued in November 2012, has informed the Department's development work in this area, and will serve as a guide for future assessments by the Privacy Office.

In this year's report, the DHS Privacy Office and CRCL present assessments of four of the Department's activities under EO Section 4(a), (c), (d), and (e). Broadly, these activities include efforts to (1) develop more efficient and effective sharing of threat information with the owners and operators of Critical Infrastructure (CI) and (2) expand DHS efforts to bring private sector experts into the Department to consult on cybersecurity issues and to expedite the processing of their security clearances. The Department continues implementation of the remaining EO requirements. The DHS Privacy Office and CRCL will assess those activities, and provide updates as needed on the assessments below, in future reports.

Recommendations

In the assessments that follow, the DHS Privacy Office and CRCL present seven recommendations to enhance the privacy, civil rights, and civil liberties protections already in place in the activities the Department is undertaking pursuant to Section 4 of the EO. Each assessment includes recommendations specific to that assessment. In addition, the Offices recommend that the Department, in the interest of transparency and consistent with its history of proactive public engagement on cybersecurity matters, make public the policies and processes it has developed to implement EO 13636, to the greatest extent possible.

[14] These PIAs and links to associated SORNs are available on the DHS Privacy Office's website at http://www.dhs.gov/privacy-documents-national-protection-and-programs-directorate-nppd.

[15] The DPIAC is a discretionary advisory committee established under the authority of the Secretary of HomelandSecurity in 6 U.S.C. § 451. The DPIAC operates in accordance with the Federal Advisory Committee Act, 5 U.S.C. Appendix 2. More information about the DPIAC, including all reports and recommendations, is available on the DHS Privacy Office website at http://www.dhs.gov/privacy-office-dhs-data-privacy-and-integrity-advisory-committee.

II. EO Implementation Activity: Cybersecurity Information Sharing through Sharelines

EO Section 4(a):

> *It is the policy of the United States Government to increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities so that these entities may better protect and defend themselves against cyber threats. Within 120 days of the date of this order, the Attorney General, the Secretary of Homeland Security (the "Secretary"), and the Director of National Intelligence shall each issue instructions consistent with their authorities and with the requirements of section 12(c) of this order to ensure the timely production of unclassified reports of cyber threats to the U.S. homeland that identify a specific targeted entity. The instructions shall address the need to protect intelligence and law enforcement sources, methods, operations, and investigations.*

Description

To enable an increase in the volume, timeliness, and quality of unclassified cyber threat reports disseminated by the Department, DHS will produce and use "Sharelines." Meant for broad dissemination, a Shareline is an unclassified and less-restrictive portion or excerpt of a report or other information source that provides the substance of a dissemination-controlled report. Sharelines thus maintain protections for intelligence and law enforcement sources, methods, operations, and investigations, as well as privacy, civil rights, and civil liberties. Sharelines are comparable to tearlines developed by elements of the Intelligence Community, but they differ in that Sharelines are not governed by tearline procedures in Intelligence Community Directive (ICD) 209, *Tearline Production and Dissemination*.[16]

In June 2013, then-Secretary of Homeland Security Janet Napolitano issued a memorandum to the Department entitled "Departmental Cyber Threat Information Sharing Procedures" (Section 4(a) Memorandum). This memorandum: (1) creates the Shareline, a new DHS product with uniform standards that DHS Components will use to provide unclassified cyber threat reporting to targeted private sector entities; (2) outlines some specific protections for privacy and civil liberties; and (3) requires that DHS Components will also share any externally disseminated Shareline with NPPD and the Office of Intelligence and Analysis (I&A) within DHS.

The Department intends to further refine the Shareline process in a formal Directive and Instruction. The Privacy Office and CRCL are involved in the development of the Directive and Instruction, and those documents and that process will be the subject of the future assessments required under the EO.

[16] A tearline is a portion of an Intelligence Community-produced report or product that provides the substance of a more highly classified or controlled report without identifying sensitive sources, methods, or other operational information. Tearlines release classified intelligence information with less restrictive dissemination controls, and, when possible, at a lower classification. More information about ICD 209 may be found at http://www.dni.gov/files/documents/ICD/ICD%20209%20Tearline%20Production%20and%20Dissemination.pdf.

ITF Working Group–Cybersecurity Information Sharing Working Group

Responsibility for addressing EO Section 4(a) was assigned to the ITF Cybersecurity Information Sharing Working Group (ISWG), which was led by I&A and NPPD. Working Group participants included more than a dozen federal departments and agencies, including the Office of the Director of National Intelligence (ODNI), various DHS Components and offices, and private sector representatives.

The DHS Privacy Office, NPPD's Office of Privacy, I&A's Privacy Officer, and the DHS CRCL attended Working Group meetings and consulted with DHS participants with program responsibilities for Sharelines to develop the deliverables, and provided substantive input on all drafts.

Deliverables

- DHS Memorandum from Rand Beers, then-Acting Deputy Secretary, to Lisa Monaco, Assistant to the President for Homeland Security and Counterterrorism, entitled "Progress on Executive Order 13636 Requirement Cybersecurity Information Sharing," June 12, 2013.

- DHS Memorandum from then-Secretary Janet Napolitano entitled "Departmental Cyber Threat Information Sharing Procedures," June 17, 2013 (Section 4(a) Memorandum).

DHS Role in Sharing Cyber Threat Information

DHS derives cyber threat information in the conduct of its mission, which includes protection of federal civilian networks, outreach to the private sector, law enforcement activities, cyber threat analysis, and risk mitigation assessments. DHS Components use a variety of methods to share cyber threat information with private sector and government entities, including systems and programs run out of the National Cybersecurity and Communications Integration Center (NCCIC), a 24-hour information sharing, analysis, and cyber and communications incident response center that serves as a DHS (and frequently a U.S. Government) focal point for cyber and communications security-related information sharing.

Under the Section 4(a) Memorandum, any DHS Component that gathers, receives, analyzes, produces, or discloses dissemination-controlled reports concerning cyber-related threats specific to a targeted entity, except those reports originating in a non-DHS element of the Intelligence Community, will develop Sharelines in accordance with the procedures established in the Section 4(a) Memorandum. Moreover, DHS Components will provide Shareline reports to I&A and NPPD – as the centralized managers of the processes under the Section 4(a) Memorandum – for dissemination throughout DHS, as appropriate.

Privacy and Civil Liberties Protections

DHS's Section 4(a) Memorandum establishes explicit FIPPs-based privacy protections, as well as civil liberties protections:

- Sharelines will render facts and judgments consistent with the original information on which they are based.
- Sharelines will be developed with the expressed intent of sharing reporting with relevant targeted private sector entities, as well as authorized government recipients with authority to act upon such information.
- Sharelines will be prepared for the broadest possible readership while protecting privacy, civil rights, and civil liberties.
- Sharelines will clearly indicate the permitted distribution of content contained within the Shareline portion, using appropriate terminology and designators … that clearly and effectively limit dissemination of sensitive information to specific targeted entities.
- Sharelines will minimize PII of individuals, except when the named individual consents to disclosure or when the disclosure would be operationally necessary to characterize a threat and otherwise consistent with the Privacy Act and all other applicable policies, procedures, and guidance concerning disclosure of PII outside the Department. In addition, the following information must be minimized:
    - Other sensitive information that is potentially attributable to an individual, including, but not limited to, privileged or legally protected content, such as attorney-client communications, First Amendment-protected materials, educational or medical records, or any content pertaining to other evidence of constitutionally protected activities.
    - Any commercial information unrelated to the cyber threat which, if disclosed, could reasonably be expected to alter the legal, commercial, or reputational standing of entities, such as legally privileged information, trade secrets, research and development information, or financial information.

In addition to these protections referenced in the Section 4(a) Memorandum, there are additional protections that are required of all DHS activities involving PII, including cybersecurity activities and threat reporting. The DHS Privacy Office ensures that these protections are in place by examining these and other programs through our Privacy Compliance, Oversight and Review, and Policy processes.

The Privacy Office and CRCL also have an additional operational role to ensure privacy, civil rights, and civil liberties are protected in certain products and threat reporting disseminated by I&A. Under I&A Policy Instruction 901,[17] for example, both offices currently review I&A

[17] *DHS Intelligence and Analysis Review and Clearance of Analytic Products Disseminated Outside the Federal Government*, April 2013.

intelligence products "originally intended for dissemination to non-DHS federal government entities and repurposed for dissemination to… private sector entities…" before they are released to ensure the draft product is consistent with all privacy, civil rights, and civil liberties policies and standards. Similarly, the Privacy Office and CRCL will work with other DHS stakeholders to develop an appropriate protocol for oversight of Sharelines.

Privacy Compliance Documentation

All cybersecurity activities at DHS must be consistent with privacy law and DHS privacy policy, including the existing DHS sharing programs that will be leveraged in the creation of Sharelines. This compliance with privacy law and policy is effectuated following engagement with the Component Privacy Office and the DHS Privacy Office and undertaking the Privacy Compliance Process.

At DHS, the Privacy Compliance Process begins with a program filing a PTA with the Component Privacy Office for submission to and approval by the DHS Privacy Office. In collaboration with the program and Component Privacy Officers, the DHS Privacy Office uses PTAs to evaluate whether existing privacy compliance documentation (typically a mix of PIAs and SORNs) sufficiently addresses an activity's privacy impacts and to determine whether new privacy compliance documentation is needed.

DHS has published a number of PIAs related to its cybersecurity function. For instance, DHS/NPPD/PIA-026 *National Cybersecurity Protection System (NCPS)*[18] gives a general overview of what information is collected, for what purposes, and how privacy is protected in the context of cybersecurity. Other PIAs provide more specific information on a particular component of NCPS, such as EINSTEIN 1, 2, and EINSTEIN 3 Accelerated (E^3A). Not all cyber threat information held or shared by the Department is subject to the Privacy Act's SORN requirement, specifically because in certain cases information that could be considered PII that is itself cyber threat information is not retrieved by the Department by a personal identifier, and thus the Privacy Act does not apply. However, the Department issues PIAs, which provide transparency about the potential risks to privacy and steps the Department has taken to mitigate those risks.

Additional Resources

- www.dhs.gov/cybersecurity-and-privacy
- DHS Directive 047-01, *Privacy Policy and Compliance*, July 2011.[19]
- DHS Management Directive 11042.1, *Safeguarding Sensitive But Unclassified*

[18] This PIA and all others referenced in this section of the assessment are available at www.dhs.gov/cybersecurity-and-privacy.
[19] Available at http://www.dhs.gov/xlibrary/assets/foia/privacy-policy-compliance-directive-047-01.pdf.

Information, January 6, 2005.[20]

- I&A Policy Instruction 901, *DHS Intelligence and Analysis Review and Clearance of Analytic Products Disseminated Outside the Federal Government*, April 2013.
- *DHS Handbook for Safeguarding Sensitive Personally Identifiable Information*, March 2012.[21]

Privacy Risks/Impacts:

Generally, the privacy risks associated with Sharelines are small. The content of Sharelines—including any PII—will derive exclusively from existing intelligence products, threat reports, and other information that the government already collects, analyzes, and shares in support of its cybersecurity, law enforcement, and intelligence missions. By definition, no new PII will be collected and Sharelines will contain no new information, including PII, or analysis. Thus, there are no new risks stemming from collection, use, or maintenance of additional PII, though there may be some additional risk due to increased dissemination of already collected PII—a risk we address below.[22]

The Section 4(a) Memorandum creates a standard product for use by all DHS Components that have a role in cyber threat reporting. A key requirement for the standard products is that some PII and other information that may have been shared appropriately within the Federal Government must nevertheless be minimized in Sharelines. These mechanisms are privacy enhancing, further ensuring that DHS cyber threat information sharing adheres to all applicable privacy policies and standards.

Still, because the purpose of the EO and Section 4(a) is to increase the amount of cyber threat information sharing with the private sector entities operating outside of federal privacy law and DHS privacy policy, there is a modest risk that PII will be overshared in Sharelines, a risk that is amplified once the broadly disseminated Sharelines are beyond DHS's control.

Specifically, there are two types of PII potentially impacted by the creation of a Shareline product: (1) PII associated with the target of a cyber threat and (2) PII that itself may be a cyber threat indicator (*e.g.*, the cyber threat may include a particular email address that is part of the cyber threat indicator). Each is considered cyber threat information, but separate privacy considerations apply to each.

---

[20] Available at https://www.dhs.gov/xlibrary/assets/foia/mgmt_directive_110421_safeguarding_sensitive_but_unclassified_information.pdf.
[21] Available at http://www.dhs.gov/sites/default/files/publications/privacy/Guidance/handbookforsafeguardingsensitivePII_march_2012_webversion.pdf.
[22] A number of PIAs are listed within the Transparency Section below. These PIAs give an overview of the Department's existing cybersecurity activities and contain their own FIPPs analysis. The rest of the FIPPs analysis within this report is more narrowly focused on the Shareline product created under Section 4(a) Memorandum.

Thus, the FIPPs analysis that follows focuses exclusively on the potential privacy risks and mitigation strategies associated with the broader dissemination of such PII outside of DHS, as required by the Section 4(a) Memorandum.

FIPPs Analysis

Transparency:

DHS has published a number of PIAs explaining how it currently collects, uses, maintains, and disseminates cyber threat information, including any PII.[23] These PIAs provide generalized notice of DHS's cyber activities as they relate to cyber threats:

- ***DHS/NPPD/PIA-026*** National Cybersecurity Protection System (NCPS), July 30, 2012. NCPS is an integrated system for intrusion detection, analysis, intrusion prevention, and information sharing capabilities that are used to defend the federal civilian government's information technology infrastructure from cyber threats. NPPD conducted this PIA because PII may be collected by the NCPS, or through submissions of known or suspected cyber threats received by the NCCIC/United States–Computer Emergency Readiness Team (US-CERT) for analysis.

- ***DHS/NPPD/PIA-027*** EINSTEIN 3 Accelerated (E^3A), April 19, 2013. DHS's Office of Cybersecurity and Communications (CS&C) continues to improve its ability to defend federal civilian Executive Branch agency networks from cyber threats. Similar to EINSTEIN 1 and EINSTEIN 2, DHS deployed E^3A to enhance cybersecurity analysis, situational awareness, and security response. With E^3A, DHS will not only be able to detect malicious traffic targeting civilian federal government networks, but also prevent malicious traffic from harming those networks. This is accomplished through delivering intrusion prevention capabilities as a Managed Security Service provided by an Internet Service Provider (ISP). Under the direction of DHS, ISPs will administer intrusion prevention and threat-based decision-making on network traffic entering and leaving participating federal civilian Executive Branch agency networks. This PIA was conducted because E^3A includes analysis of federal network traffic, which may contain PII.

- ***DHS/NPPD/PIA-028*** Enhanced Cybersecurity Services (ECS), January 16, 2013. ECS is a voluntary program based on the sharing of indicators of malicious cyber activity between DHS and participating Commercial Service Providers (CSP). The program assists owners and operators of CI to enhance the protection of their systems from unauthorized access, exploitation, or data exfiltration through a voluntary information sharing program. ECS consists of the operational processes and security oversight required to share unclassified and classified cyber threat indicators with companies that provide internet, network, and communication services to enable those companies to enhance their services to protect U.S. CI entities. ECS is intended to support U.S. CI;

[23] Available at www.dhs.gov/cybersecurity-and-privacy.

however, pending deployment of EINSTEIN intrusion prevention capabilities, ECS may also be used to provide equivalent protection to participating federal civilian Executive Branch agencies. NPPD conducted this PIA because PII may be collected. The Privacy Office's and CRCL's Assessment of the expansion of ECS required by Section 4(c) of the EO is below.

- ***DHS/NPPD/PIA-008*** EINSTEIN 2, May 19, 2008. The original PIA for EINSTEIN 1, dated September 2004, explained that EINSTEIN 1 analyzes network flow information from participating federal civilian Executive Branch agencies networks and provides a high-level perspective from which to observe potential malicious activity in computer network traffic of participating agencies' computer networks. The updated version, EINSTEIN 2, incorporates network intrusion detection technology capable of alerting NCCIC/US-CERT to the presence of malicious or potentially harmful computer network activity in federal civilian Executive Branch agency network traffic. EINSTEIN 2 principally relies on commercially available intrusion detection capabilities to increase the situational awareness of the US-CERT.

- ***DHS/NPPD/PIA-001*** The EINSTEIN Program, September 2004. EINSTEIN provides NCCIC/US-CERT with a situational awareness snapshot of the health of the federal government's cyber space. Based upon agreements with participating federal agencies, NCCIC/US-CERT installs systems at the agencies' respective Internet access points to collect network flow data. The agencies are provided tools to analyze their collected data. In addition, the data is shared with NCCIC/US-CERT Security Operations Center, which aggregates it from all EINSTEIN participants to identify network anomalies spanning the Federal Government.

As DHS issues its forthcoming Cyber Shareline Directive and Instruction, the Privacy Office will review existing privacy compliance activities to ensure the Department is as transparent about these activities as possible.

The Department has also engaged in more direct actions in support of transparency about Sharelines. For example, the ISWG conducted three large working group meetings in 2013, to develop the concept for Sharelines and policy for implementing EO Section 4(a), engaging more than 250 representatives from DHS, the Department of Justice (DOJ), ODNI, Sector Specific Agencies (SSA), and other federal departments and agencies. In addition, the ISWG fostered transparency by holding bi-weekly meetings with the broader ITF stakeholder community, including non-federal entities and private sector participants, to update them on the status of its efforts. These updates enabled participants to understand government efforts to protect cybersecurity and CI. They also allowed the ISWG to obtain valuable feedback and insights from stakeholders, which included customers of the information to be included in Sharelines.

The ISWG also participated in the series of advocate briefings hosted by the DHS Privacy Office and CRCL. On April 24, 2013, members of the ISWG updated interested members of the privacy and civil liberties advocacy community on their activities under the EO and Presidential Policy Directive-21 (PPD-21). After the Shareline policy was signed in June 2013, the ISWG

further briefed the Shareline concept to numerous State and local entities and private sector bodies, including during a public meeting of the National Infrastructure Advisory Council.

In addition to the ISWG's outreach efforts, on September 12, 2013, the ITF Co-Chair, the NPPD Privacy Officer, and the DHS Privacy Office's Senior Director for Privacy Oversight briefed the DPIAC on the various DHS activities under the EO, including the work being done pursuant to EO Section 4.

Individual Participation:

Information about cyber threats will likely come from a variety of sources, including from individuals or entities that are targeted by cyber attacks or victimized by cyber crime. This information, when available, is collected and maintained by DHS to some extent already. The privacy interests of these individuals are protected under the Section 4(a) Memorandum's minimization procedures for Sharelines, which require DHS to obtain consent of the individual who is either a target of a threat or knowledgeable about the threat before his or her PII can be included in a Shareline report. Such consent is an important measure of ensuring Individual Participation.

Of course, an individual who is a suspected cyber threat actor, or whose PII is itself a cyber threat indicator, will not be given the same opportunity to participate in the process of determining what information about him or her is present in a disseminated Shareline about a threat, and consent will not be sought. Still, given the various layers of minimization procedures discussed below, PII about suspected cyber threat actors may not be included in the disseminated Shareline products, even when DHS or other government agencies have lawfully collected the information, when a determination has been made that the identity of the threat actor is not material to the Shareline.

Purpose Specification:

DHS components have a variety of authorities to collect and share cyber threat information, such as through their responsibilities to protect federal civilian networks, coordinate with the private sector, conduct law enforcement activities, analyze cyber threats, and perform mitigation assessments. For example, NCCIC collects cyber threat information pursuant to:

1. *Federal Information Security Management Act* (44 U.S.C. § 3546), which establishes that there will be a federal information incident security center. That center is NCCIC.

2. *Homeland Security Act of 2002 (*6 U.S.C. §§ 121 and 143), which provides requirements for alert, warning, and analysis of cyber risks and vulnerabilities to state and local government entities, crisis management support, and technical assistance to private sector and other government entities. In addition, the Act requires a comprehensive assessment of the vulnerabilities of CI and key resources of the United States and recommended measures necessary of protection.

3. *PPD-21: Critical Infrastructure Security and Resilience*, February 12, 2013, which requires US-CERT to aid DHS, other federal agencies, State and local governments, and

the private sector to identify, prioritize, and coordinate the protection of CI and key resources against terrorist attacks while protecting the civil liberties of U.S. persons.[24]

The enhanced sharing contemplated through Sharelines will be consistent with these and other existing authorities.

Data Minimization:

Before PII is included in a disseminated Shareline, it will undergo at least two independent minimization reviews. First, as Sharelines are commonly derived from other reporting that is subject to privacy and civil liberties requirements, including the procedures for minimizing U.S. Person information under Executive Order 12333, *United States Intelligence Activities*,[25] a determination whether to minimize PII will have been made before the work to derive a Shareline product is undertaken. In these cases, this initial determination to minimize the PII will control; PII will not appear in a Shareline when it was minimized in the reporting from which the Shareline is derived.

In addition, even when PII is included in the reporting that is the source for the Shareline, the Section 4(a) Memorandum requires a second minimization review. Under this review, PII must be minimized unless:

1. The individual consents to the use of his or her PII, or
2. The PII is necessary to characterize a threat and is consistent with the Privacy Act.

As noted in the discussion of the Individual Participation Principle above, the first exception will apply principally to both targets of cyber threats and the source of the government's information about the threat. In either case, the default minimization procedure is privacy protective, because the PII will not be disseminated in a Shareline unless the individual most likely to be impacted by the disclosure specifically consents to his or her PII being disclosed in a Shareline.

The second exception will generally serve to protect the privacy interests of suspected threat actors. Even without their consent, before their PII can be included in a disseminated Shareline report, a DHS analyst must determine that their PII is necessary for recipients to understand the threat.

Use Limitation:

The purpose of EO Section 4(a) is to ensure that targeted entities and other government agencies with the authority to act on cyber threat information receive notice of those threats. The Section 4(a) Memorandum requires components that generate these reports to take steps to limit the uses

[24] PPD-21 is available at http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil. PPD-21 revokes Homeland Security Presidential Directive-7 (HSPD-7): Critical Infrastructure Identification, Prioritization, and Protection, December 17, 2003, available at http://www.fas.org/irp/offdocs/nspd/hspd-7.html. Under PPD-21, plans developed pursuant to HSPD-7 shall remain in effect until specifically revoked or superseded.

[25] Available at http://www.fas.org/irp/offdocs/eo12333.htm.

consistent with these purposes. Specifically, under the Memorandum's guidance, "Sharelines will be written with the expressed intent of sharing reporting with relevant targeted private sector entities, as well as authorized government recipients with authority to act upon such information." Moreover, under the guidance "Sharelines will clearly indicate the permitted distribution of content contained within the Shareline portion, using appropriate terminology and designators … that clearly and effectively limit dissemination of sensitive information to specific targeted entities."

These requirements help the government limit the use of PII through targeted dissemination to relevant parties only. In addition, since recipients will either be targeted entities or government agencies with the responsibility and ability to act on such information, their use is naturally limited to crafting authorized responses to the threat reported in the Shareline. The required distribution and sensitivity markings will further assist recipients to identify when they receive sensitive information, including PII, as part of a Shareline report.

Data Quality and Integrity:

Sharelines are derived from existing threat and intelligence reporting, and the data quality and integrity measures in place for those activities, as set forth in the various PIAs listed above, flow through to the creation of Shareline products.

The Section 4(a) Memorandum reinforces this connection by requiring that "Sharelines render facts and judgments consistent with the original information on which they are based." This ensures that the information in the Shareline—including whatever PII has not been minimized—relates to the threat reporting or intelligence it is based upon, with no new conclusions, assertions, or other link to derogatory information.

Security:

There are no new Security requirements placed on the Department under EO Section 4(a), as the creation of Sharelines follows existing processes for handling cyber threat information, which are described in the various PIAs listed above. Many of these existing processes follow strict security and handling requirements for law enforcement sensitive and classified national security information.

Accountability and Auditing:

The Section 4(a) Memorandum will enhance Accountability and Auditing by establishing a uniform process for issuing Sharelines. The required distribution and sensitivity determinations and markings in the Shareline product (discussed in the Use Limitation Section, above), help recipients in DHS and the private sector identify the nature of the information in the product and understand their obligation to protect it.

Civil Liberties Considerations:

The Potential for Over-Sharing

Generally, the civil liberties risks associated with Sharelines are moderate because the great majority of cyber threat information contained in administrative, law enforcement, or intelligence systems and likely to be shared is purely technical in nature, with no nexus to PII or individuals, or commercial entities. Some of the cyber threat information, however, does contain information tied to individuals and entities. This sharing process therefore needs to be carefully developed in order to avoid posing a risk to the rights of those individuals or entities.

The potential risk to individual rights stems from the nature of information retained in the government's data systems. As noted above, most of the cyber threat information retained by the U.S. Government is technical in nature, but some PII, Sensitive PII,[26] and other potentially sensitive information may be retained, either incidentally or because it is directly relevant to the detected cyber threat. This information is present in U.S. Government record systems only as a consequence of association with a particular cyber incident, a cybercrime, or actions taken by an adversary, but may not always be threat information itself. The risk to individual rights stems from the possibility that the Department could potentially "over share" threat-related or incidentally collected information, and that disclosure could have an adverse effect on the individuals whose information was shared.

There are many systems and processes for the collection, retention, sharing, and dissemination of cyber threat information. How the information is used and shared (appropriately, and in compliance with applicable laws and policies) across the entire U.S. Government enterprise is staggeringly complex, and what is done and how it is accomplished in any particular instance depends on many variables. A detailed exploration of those systems and processes is beyond the scope of this document, so the focus of the assessment will be on high level policy principles.

CRCL views over-sharing as the primary risk associated with Sharelines because the government retains considerable amounts of data, and much of it is sensitive. The promulgator of the Shareline may be focused on sharing as much information as possible rather than also weighing the interests of those who may be affected by a disclosure. When a cyber incident occurs, particularly a high profile incident that is prominently featured by the media, it is common for CI operators to request detailed information from DHS about the incident in order to better defend their own networks, and to ascertain whether their own defenses respond to well-publicized threats. CRCL believes that the risk of sharing more information than is necessary poses the most likely threat to individual rights in the Sharelines context because it is a reasonably foreseeable error, of a type that is common in government and business, and it does not require mal-intent or extraordinary effort to occur.

[26] Sensitive PII is PII that, if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. *DHS Handbook for Safeguarding Sensitive Personally Identifiable Information*, March 2012, available at http://www.dhs.gov/sites/default/files/publications/privacy/Guidance/handbookforsafeguardingsensitivePII_march_2012_webversion.pdf.

How Cyber Threat Information Is Collected, Retained, Shared

To fully understand the potential risk to individual rights and how the Department is working to address the risk, it is necessary to consider how and why cyber threat information is collected, and what types of information are possessed by the Department. A hypothetical law enforcement investigation may be useful to illustrate how DHS and other U.S. Government agencies work together to address cyber incidents, and how that affects data handling at DHS.

The victims of a cybercrime may contact a hypothetical law enforcement agency for assistance. That agency will likely look to the affected computer system to detect and gather evidence of the incursion, to identify the perpetrator, to develop investigative leads, and to analyze exactly what occurred at a technical level in order to better detect future crimes.

The agency's investigation may require only a limited inspection of a small part of the affected system, or it may require a much more detailed, long-term forensic examination of a considerable portion of the system, either on the original hardware, or on a mirror image of a hard drive, server, thumb drive, or other media. The agency may need technical assistance in its forensic examination, and the victim may need help to restore its system, so some information may be shared with other federal agencies that have unique expertise in those areas. At the same time, the investigation may uncover evidence of a hostile nation-state actor's involvement in the incident, terrorists, or a crime involving another agency's specialized jurisdiction. The law enforcement agency will share enough information to enable the technical experts to provide assistance, and it will share other information about the incident with relevant authorities. Additionally, information about the exploit may be shared with other government agencies to warn them about this new threat.

After the investigation runs its course, the law enforcement agency may want to retain–per applicable laws, regulations, policies, and records schedules–some of that information for use in analyzing future threats, and to meet administrative record keeping requirements. The information may be examined in the future by other cybersecurity experts who have a need to know, in an effort to build cases against criminals or to understand new cyber threats.

The nature of information examined by this law enforcement agency and subsequently retained in government records at that agency and others varies greatly, and is context-dependent on the cyber threat, and on the agency's particular mission needs. Cyber threat information predominantly involves computer code, IP addresses, and other detailed information about how a particular piece of malware or a particular scheme exploits specific vulnerabilities in software, systems, or operator behavior. Other elements of information, however, may be necessary to identify, characterize, and respond to a particular threat, while some elements of information may be retained because it is not practical to separate them from the point of the cyber attack.

It may be helpful to think about the types of information retained as *direct* evidence of a cyber threat (things the adversaries did), *related* information (from or about the victims, which shed light on the incident), and *incidentally retained* information relating to individuals or entities who were not a target of the attack, but whose data or systems were in close proximity to it. These terms should not be viewed as a complete list of the types of information that may be

captured in response to a cyber incident, but rather as a construct to help conceptualize what kinds of information may be involved.

The *direct* evidence of a cyber threat may include artifacts of the threat itself, such as a piece of malware, spoofed email or domain name service addresses, or a spearphishing email. It may also include evidence of the intrusion into the system. This evidence would be revealed by audit trail information showing when and where a system was accessed, what files were downloaded, what portions of the system were accessed, whether any additional equipment was connected to the exploited system, and similar records of the adversary's activities. Direct evidence of the cybercrime is often not found in a single place on a disc or in memory, but may be scattered on a hard drive or in a bank of servers. A forensic examination of a hard drive may require the presence of all the information on that hard drive in order to find all the scattered evidence showing how the malware exploit worked, and how to stop it in the future.

Information about targets or victims of the exploit (*i.e.*, those directly affected by it) is considered *related* information. Related information may be retained to document the incident, to help with analyzing the adversary's actions or innocent actions (such as opening a bad attachment) that had something to do with the incident. Such information may include data inside systems, such as copies of the information or files stolen from the victim, information about the victim's normal activities on the system, how the victim's system was configured, what hardware and software was present, and so forth. Additional information may be sought from the victim as additional evidence of an incident or as a method of putting the cyber incident in context. Criminal investigators, for instance, may look for information showing a pre-existing tie between the victim and the adversary (such as prior employment status), while an agency providing technical assistance may look to find out who among a long list of employees clicked on a particular link in a spearphishing email. The types of *related* information that may be collected in response to an incident may be more numerous and wider-ranging in nature than *direct evidence* of the incident.

Finally, some information that is only *incidentally* present at the "scene" of a cybercrime or cyber incident may need to be retained, either because it cannot reasonably be separated from the direct evidence and related information, or because it may also shed a light on the adversary's actions. For example, the hypothetical investigating agency may need to take or image multiple server blades in order to fully examine how the cybercrime occurred, including consideration of the system's configuration, what security measures were in place, and whether other individuals or entities in close digital proximity (*e.g.*, hosted within the same server farm) were targets or co-conspirators. Such information is sometimes collected and retained when it appears to be potentially relevant but the relevance cannot immediately be ascertained, or more likely when it is not practicable to segregate it from the direct evidence of the cyber incident, and related information. In comparison to the *related* information, the *incidentally retained* information is even more extensive than related information.

Government cybersecurity professionals make efforts to limit the amount of information collected and retained. In addition to policies governing their activities, collecting unnecessary data is unlikely to advance an investigation or technical assistance effort, and may in fact hinder it. There are compelling operational reasons, therefore, to minimize information, and the

collection of useful technical data, the *direct evidence* of a cyber incident and how it occurred, will generally be the goal, but the fact remains that *related information* and *incidentally retained* information are still lawfully and legitimately present in some government systems, and need to be properly accounted for and governed in any cyber threat information sharing activity.

Use and Protection of Individual and CI Entity Data

Individual rights may be affected by the Department's retention and sharing of data, but it is hard to prospectively determine which rights may be affected, because the rights implicated vary depending on the nature of the data retained, its sensitivity, and how it is used. Many measures are in place to protect individual rights and the CI entities' interests when the information is retained, used, and disseminated in federal data systems, but there is no single overarching federal standard. Each government agency is obligated to collect, retain, use, disseminate, or expunge the shared information in accordance with the laws, regulations, policies, and record schedules governing their respective activities.

Not all protections directly depend on the regulations and policies governing particular data systems. Some federal standards indirectly protect individual rights and CI entities' interests. For example, the national security classification system was established to protect information, the release of which could harm national security. In addition to protecting sensitive sources, methods, and information, it maintains information in confidence, protecting the privacy (and in some instances commercial interests) of those individuals and entities that appear within classified record systems. Similarly, information about cyber incidents may at times be provided to DHS under a promise of confidentiality, such as the categorical exclusion of the Protected Critical Infrastructure Information (PCII) scheme. This statutory scheme, enacted to encourage exchanges of CI vulnerability information between CI entities and the U.S. Government, may also be used to protect the victim, the affected CI entity, and the interests of innocent third parties whose data has to be shared in order to effectively address a cybersecurity threat directed at CI.

Considerable amounts of data may appropriately be retained during the course of these agencies' duties, and some of that information may presently be shared–generally in minimized form–in products warning about cyber threats, or in efforts to make sense of new, emerging cyber threats. The Sharelines products will increase information sharing with CI entities, but that sharing must still be done responsibly and in accordance with all applicable protections of individuals' (and entities') rights.

The DHS Shareline Standard

There is no single federal standard describing what types of cyber threat information need to be shared among government agencies to ensure that appropriate information is ultimately shared with CI entities. Given the need for increased sharing of threat information, we anticipate that agencies are likely to share potential threat information as broadly as possible within the Federal Government, and trust the gatekeepers at the SSAs (and DHS in particular, with respect to Sharelines) to exercise good judgment about what information can be shared with CI entities.

The potential clearly exists for the improvident release of PII, Sensitive PII, or other sensitive information, which could in turn cause damage to individuals or entities. The standard prescribed in the Section 4(a) Memorandum, works to mitigate these risks by directly addressing the need for civil liberties protections, and by articulating a more specific standard that should be broadly applicable across a wide range of cyber threat sharing activities.

By way of general guidance, the Section 4(a) Memorandum directs that "Sharelines will be prepared for the broadest possible readership while protecting privacy, civil rights and civil liberties." The Memorandum then prescribe a minimization standard to protect privacy and civil liberties:

> *Sharelines will minimize personally identifiable information (PII) of individuals, except where the named individual consents to disclosure or where the disclosure would be operationally necessary to characterize a threat and otherwise consistent with the Privacy Act and all other applicable policies, procedures, and guidance concerning disclosure of PII outside the Department.*

This standard–which could be paraphrased as "minimize unless necessary to characterize a threat"–offers basic protection for privacy and civil liberties. It directs that PII, Sensitive PII, or other information that could be tied to an individual be minimized unless the individual has consented to disclosure, or when the only way to characterize the threat is to disclose that information.

The exception to the minimization requirement–for purposes of accurately describing the threat–is necessary because not all threats may be readily characterized by a purely technical description such as computer code or a malware signature. For example, a spearphishing attack may originate in the hacked email account (or spoofed email address) of a bank president. The malicious email may feature some details about the bank president and his business to lend the email authenticity and to encourage an unwitting recipient to open a malware attachment or click on a hypertext link to a malicious website. In some instances, there may be no other indicators associated with the threat that would permit the efficient detection and interdiction of a spearphishing email. Cybersecurity personnel would be compelled to rely on the spoofed or hijacked email address and the communicative content associated with the exploit in order to address the threat.

CRCL does not anticipate that PII, Sensitive PII, or other sensitive information will be routinely shared under this exception. In our experience, such sharing is generally not necessary to address most threats. The standard does allow these exceptions, however, because the gravity of a particular threat may compel DHS to share as much of the information as is needed to characterize the threat. Even so, the standard still requires the Shareline to minimize such information as much as possible, with no more information than is necessary to describe the threat in a way that allows recipients to effectively respond to the threat.

As noted above, the rights implicated in any collection of cyber threat data depends on the nature of the materials collected. As cybersecurity threats generally target communications systems, malware can be intermingled with communicative content that individuals and CI entities use to

accomplish things–to obtain health care, to service debts or invest money, communicate with educational institutions, to air grievances, to communicate with legal counsel, to file patents, to conduct research, and develop business processes. The list of rights potentially affected by government examination of a CI entity's computer network is potentially open-ended, with one feature in common: all of these rights and interests are secured by due process. That principle in some instances gives effect to specific fundamental rights or statutory protections, or in the absence of those specific protections, acts as a check on injurious Government action, offering those whose interests are injured by the government legal means of redress for the injury, so at a minimum the Government is obliged to exercise a standard of reasonable care with respect to this information.

The Section 4(a) Memorandum addresses this complexity by applying the same minimization standard to other types of information that a cybersecurity, law enforcement, or intelligence professional should be able to recognize as sensitive information:

> *In addition, the following information must be minimized:*
>
> - *Other sensitive information, that is potentially attributable to an individual, including, but not limited to, privileged or legally-protected content, such as attorney-client communications, First Amendment-protected materials, educational or medical records, or any content pertaining to other evidence of constitutionally-protected activities; and*
>
> - *Any commercial information unrelated to the cyber threat which, if disclosed, could reasonably be expected to alter the legal, commercial, or reputational standing of entities, such as legally-privileged information, trade secrets, research and development information, or financial information.*

This standard addresses the treatment of two types of individual rights-sensitive information within Sharelines: information relating to individuals, and information relating to CI entities. While individuals clearly enjoy constitutional protections and other legal protections regarding their communications, the precise extent of protections enjoyed by CI entities is not clear, due to both the widely varying nature of communications retained in CI entity systems, and also a paucity of constitutional case law. Rather than trying to ascertain the appropriate minimal legal floor for the treatment of CI entity information, the Procedures, therefore, treat CI entity information comparably to individual information, applying a higher standard of care.

It is not feasible to try to anticipate all the types of information that may be incidentally associated with cyber threats. The standard is therefore written in an open-ended manner. Individual communications, "*including, but not limited to*" the short exemplary list of individual rights-related communications, are protected. Similarly, the commercially sensitive (and in some instances legally protected) communications likely to be found at some CI entities is covered in the second bullet item, along with a catchall standard covering, "*which, if disclosed, could reasonably be expected to alter the legal, commercial, or reputational standing of entities.*" In

effect, this applies a single standard–the higher standard of care enjoyed by individuals–to both categories of information.

The standard protecting individual rights is intuitive. An exhaustive list is not feasible, so a short list of the most likely individual rights-sensitive communications is cited to provide an example, and in effect a duty is imposed on DHS personnel to exercise common sense to identify any other information that may be comparably sensitive, and treat it accordingly. Most cyber threat information is technically focused, and CRCL believes that this standard, diligently applied, should be sufficient to mitigate the moderate risks posed to individual rights by the expanded information sharing envisioned for Sharelines.

The standard respecting the rights and interests of CI entities functions similarly, but it serves multiple interests in addition to protecting legally cognizable rights. First, it respects the rights and interests of the CI entity that (likely) reported the cyber incident, treating that information comparably to information that contains incidentally collected content relating to the exercise of individual rights. Second, it further requires that the proponents of a Shareline product respect the rights and interests of other CI entities, requiring that information be redacted if it could harm "*entities*," not just a particular CI entity mentioned in the cyber threat information. That requirement will likely protect any CI entities mentioned in the Shareline, while also working to avoid harm to any other CI entities.

The standard respecting the rights and interests of CI entities responds to some CI entities and critics, who have expressed a two-fold concern: that publicly sharing cyber threat information may cause repercussions in the marketplace against CI entities that report cyber incidents; and that U.S. Government disclosure of cyber threat information may affect the competitive balance of all participants in a given marketplace. For instance, the public disclosure of information about an incident (such as a data breach or detected financial fraud) could significantly harm the well-meaning CI entity that reported the incident. If the disclosure contains information about other competitors having been victimized, it could harm them as well. CRCL believes that this measure adequately addresses both concerns at this time.

Recommendations

1. The Department should give consideration to requiring a review or audit of Sharelines by the DHS Privacy Office, CRCL, and other oversight offices. This will enhance the Principle of Accountability and Auditing in service of the rest of the FIPPs implemented in support of this activity. An appropriate review regime would provide a means of ensuring compliance with the Procedures and the pending Directive and Instruction, and ensuring privacy and civil liberties oversight in Sharelines.

2. DHS should establish specific procedures to encourage Shareline recipients to limit their use of information contained in a Shareline to that which is necessary to respond to the threat, including limiting onward dissemination of any PII, Sensitive PII, or other sensitive information contained in the Shareline report. This recommendation will support the Security and Use Limitation Principles.

3. Sharelines that include PII, Sensitive PII, or other sensitive information should include a statement notifying recipients that the product contains information that should be protected from further disclosure unless it is necessary to respond to the reported threat. This recommendation will support the Security and Use Limitation Principles.

4. Generally, the Department should continue to work with the DHS Privacy Office and CRCL as it develops the forthcoming Directive and Instruction on Sharelines, and components creating Sharelines should work with the Privacy Office to ensure their activities are consistent with existing privacy compliance requirements, protective of individual rights, and managed in ways consistent with good oversight practices.

5. DHS should develop a tracking mechanism for Shareline dissemination, leveraging the processes developed under EO Section 4(b). This will enhance the Accountability and Auditing Principle, which can reinforce implementation of the rest of the FIPPs.

III. EO Implementation Activity: Expansion of the Enhanced Cybersecurity Services Program

EO Section–4(c):

> *To assist the owners and operators of critical infrastructure in protecting their systems from unauthorized access, exploitation, or harm, the Secretary [of Homeland Security], consistent with 6 U.S.C. 143 and in collaboration with the Secretary of Defense, shall, within 120 days of the date of this order, establish procedures to expand the Enhanced Cybersecurity Services program to all critical infrastructure sectors. This voluntary information sharing program will provide classified cyber threat and technical information from the Government to eligible critical infrastructure companies or commercial service providers that offer security services to critical infrastructure.*

ITF Working Group

As this task entailed expansion of an existing and well understood DHS program, it was accomplished at the direction of then-Acting Deputy Secretary Rand Beers, without assignment to an ITF WG.

DHS Role

The Office of Cybersecurity & Communications (CS&C) within DHS/NPPD is the executive agent for the Department's activities under the ECS Program. In this capacity, CS&C:

- Collects and disseminates cyber threat information to participating CSPs;
- Manages CSP participation in the ECS program, including validating that candidate entities are owners or operators of systems or assets that meet the legal definition of United States Critical Infrastructure and therefore are eligible to participate, and the development and execution of requisite Memoranda of Agreement with CSPs;
- Provides CSPs with technical expertise regarding the use and protection of government furnished information (GFI), including review and security approval for the ECS services/countermeasures that can utilize GFI, consistent with the security requirements; and
- Works with cybersecurity organizations across the USG to gain access to a broad range of sensitive and classified cyber threat indicators in support of program execution and characterization of the risks and threats unique to CI sectors.

In addition, DHS coordinates with 16 SSAs, including the Departments of Agriculture, Defense, Energy, Treasury, Interior, Health and Human Services, and the Environmental Protection Agency, to provide recommended actions and processes for SSAs to use in support of:

- Characterizing risks and threats unique to specific CI sectors;
- Support the validation of proposed CI entities; and
- Communicating ECS program goals and parameters within their sectors.

How ECS Functions

CI Entities: Those entities seeking to participate in ECS should first contact a CSP. The DHS ECS program will make a determination of eligibility for participation (or "validation"). DHS evaluates the applicant and confirms it is an owner or operator of CI systems or assets (or "validates" it), rendering it eligible to participate in ECS. The validated entity may then negotiate to purchase cybersecurity services from a CSP.

CSPs: To participate in ECS, the aspiring CSP must apply to DHS, enter into an MOA, and meet security requirements set forth by the ECS program and other providers of sensitive cyber threat indicators included as GFI. CSPs are not required to be ISPs. A separate class of CSP (Operational Implementer, or OI) has been established for those validated CI entities that wish to provide cybersecurity services to themselves, without the use of an outside contractor CSP. The OIs must be both validated as owners or operators of CI, and meet the same requirements as a CSP.

Once vetted and approved for participation, CSPs are required to enter into a MOA with DHS. In the MOA, the CSP must agree to handle, use, and maintain all sensitive and classified information in accordance with government-provided security requirements, and to provide cybersecurity services to validated CI entities. Once a CSP is participating in ECS, it will be permitted to commercially provide cybersecurity services based on the GFI to validated CI entities. Although CSPs provide cybersecurity services, they remain free to opt out of employing particular threat indicators and coupled countermeasures.

Provision of GFI to CSPs: The ECS Program will furnish sensitive and classified government information about threats of particular concern to CI entities to the CSPs.

The selection of threat information for provision to the CSPs occurs as a routine matter at the operational level within CS&C acting in concert with government partners and may take into account input from CSPs, or any other sources of information available to CS&C. When a CSP provides feedback on the effectiveness of the threat information, the ECS Program will analyze that and take feedback into account when "refreshing" the set of threat indicators provided to the CSPs. The pairing of countermeasures with particular threat indicators occurs via an internal, interagency deliberative process involving DHS and other government agencies that provide cyber threat information. Other than requiring that CI entities be validated by DHS prior to participation, the CSPs can only provide approved ECS services/countermeasures utilizing the GFI data.

The U.S. Government is not involved, does not interfere in, or control the relationship between the CSPs and the CI entities.

Cybersecurity Monitoring and CSP Reporting to DHS: The CSPs providing ECS services on behalf of their clients, the CI entities, and that relationship is governed by a contract between the CSP and the CI entity. When an identified threat that is the subject of GFI is encountered, the CSP notes the "fact of" its detection, and the CI sector in which the threat was detected, along with the date and time encountered, and the port that was targeted. This limited, anonymized information is then aggregated and periodically reported back to DHS to provide an operational and programmatic metric–but only if both the CSP and the CI entity client agree to voluntarily provide it to DHS. The CSPs are precluded from providing additional information about their client CI entities by the terms of the MOA between DHS and the CSP.

From time to time, a CI entity participating in ECS might voluntarily decide to approach DHS or any other government agency to share additional information regarding an incident detected as a result of ECS (or through any other means), to seek technical assistance or obtain other help in responding to a cyber incident, or for any other reason. These interactions – part of ordinary interactions between DHS and CI actors – are not affected in any way by ECS. Any such additional sharing of information with the Government occurs strictly at the discretion of the CI entity, and the CI entity's decision to provide that information (or request for assistance) occurs outside of the scope of routine information sharing envisioned under ECS and outside the scope of the ECS program. The ECS program does not solicit additional information, or make any effort to direct the actions of CI entities to share information outside of ECS.

Subsequent DHS Sharing of Information Received Under ECS: DHS receives aggregated, anonymized information about the threats detected, and the CI sectors in which the threats were detected as a result of operating ECS. CS&C will share information it receives regarding cyber threats under ECS consistent with its existing policy and procedures, including sharing with other U.S. government entities with cybersecurity responsibilities. DHS shares information with its partners in order to provide shared awareness of threats to CI and to allow CI partners to better protect themselves against cyber threats.

Privacy and Civil Rights and Civil Liberties Participation

CS&C is supported by CRCL, the NPPD Privacy Office, and the DHS Privacy Office. The two privacy offices collaborated to conduct and publish the ECS PIA and continue working together to identify and mitigate privacy risks. All three offices reviewed the deliverables under this section of the EO as well. The three offices regularly provide policy advice to NPPD elements, including the ECS Program Operations (NCCIC/US-CERT) and the ECS Program Management Office. The NPPD Privacy Office and CRCL also participate in the program's deliberative process, ensuring that privacy and civil liberties are protected in the provision of GFI provided to CSPs and in the approved services/countermeasures.

Deliverables

- DHS Memorandum from Rand Beers, then-Acting Deputy Secretary, to Lisa Monaco, Assistant to the President for Homeland Security and Counterterrorism, entitled "Progress on Executive Order 13636–Establishing Procedures to Expand Enhanced Cybersecurity Services," June 12, 2013.
- Validation Criteria for Enhanced Cybersecurity Services Participation 2.1, November 13, 2013.

Privacy Compliance Documentation

- PIA
  - DHS/NPPD/PIA-028 "Enhanced Cybersecurity Services (ECS)," January 16, 2013. Available to the public at www.dhs.gov/privacy.
- SORN
  - DHS/ALL–002 Department of Homeland Security (DHS) Mailing and Other Lists System, November 25, 2008, 73 FR 71659. Available to the public at www.dhs.gov/privacy.

Additional Resources

- An ECS Fact Sheet will be posted on the DHS website later this year.

Privacy Risks/Impacts

By design, the ECS Program and its expansion under Section 4(c) of the EO, have little impact on privacy, and do not include government access to private communications.

Broadly understood, there are two categories of PII that could be obtained by the Department in this program. The first is the information collected about participating CSPs and private sector companies, each of which volunteer for the program and meet the established validation criteria established by the Department. DHS will make minimal use of PII collected from participants, and will not share it unless it meets one of the routine uses in the DHS/ALL–002 SORN.

The second category is information that could be considered PII and is itself a threat indicator. Certain indicators of a cyber threat can be the same type of information individuals use to identify themselves in online communications, such as an email address or an IP address and domain information. In the context of ECS, this type of information is involved, not because it identifies an individual, but as a reference point for particular known or suspected cyber threats. For example, a threat actor may co-opt an individual's email account and send malicious code

disguised as a message from that individual. In this instance, one of the threat indicators may include that individual's email address. However, the intent of sharing the email address is not to identify the individual; rather, it is solely used by ECS to understand the threat and alert participants of the threat coming under cover of that email.

Even so, in cases in which threat indicators contain such information, CS&C follows established Standard Operating Procedures (SOP) and cybersecurity information handling guidelines to minimize sharing PII to that necessary to understand and respond to the threat. Specifically, these procedures require CS&C to review data and information that it intends to disseminate to determine whether the information contains PII incidentally present during the investigation, research, and creation of CS&C reports or other products. Under the SOPs, an analyst will overwrite, redact, or replace information that is not necessary to understand the analysis or product.

FIPPs Analysis

Transparency:

On January 16, 2013, DHS published the PIA for the Enhanced Cybersecurity Services (DHS/NPPD-028), which is available online at www.dhs.gov/privacy. This PIA contains a full description of the program and describes how privacy risks are mitigated by implementing the FIPPs.

In addition to the PIA, the ECS program staff has done a great deal of work in support of transparency. The ECS program has:

- Created the ECS Website, which can be found at: http://www.dhs.gov/enhanced-cybersecurity-services;
- Conducted briefings to the following groups on the ECS program, each highlighting the role of privacy and civil liberties protections in ECS:
    - Information Sharing and Analysis Centers, Sector Coordinating Councils, and SSAs
    - Over 100 individual briefings with interested CI companies.
- On May 8, 2013, NPPD also briefed ECS Expansion to the privacy and civil liberties advocates meeting hosted by the DHS Privacy Office and CRCL.

Individual Participation:

Participation in the ECS program is voluntary. Information about participants, including all PII, is supplied by the participating CSPs themselves.

Before a CSP may participate, it must enter an MOA with the Department. These MOAs for Information Sharing For Enhanced Cybersecurity Services detail the roles and responsibilities of

the parties, ensuring the participating CSPs fully understand the extent of their voluntary participation.

Threat indicators are not collected with the knowledge or consent of the individual they purport to be about. In fact, an email address or other information contained in a threat indicator may not be associated with a real individual, but may instead be falsified information assembled by an adversary. It is difficult, and frequently impossible, to ascertain whether such information associated with threats is also associated with an actual person. When such information is disseminated, it is because it is known to be associated with specific threats, and it is provided to CSPs solely for the purpose of enabling the CSPs to identify threats within their or their customers' networks. Such information is not intended to identify or be linked to an actual individual, and to the extent it does, that individual has been linked to a particular cyber threat. Therefore, the principle of Individual Participation has little relevance to this particular category of information.

Purpose Specification:

ECS is being conducted pursuant to authority derived from the Homeland Security Act, 6 U.S.C. §§ 121(d), 133(g), 143; Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, § 4(c), and Presidential Policy Directive 21, Critical Infrastructure Security and Resilience.

The relationship between CSPs and DHS will be governed through the ECS MOA and the relationship between CSPs and participating entities will be governed through commercial agreements. CS&C is not a party to those agreements.

Data Minimization:

PII collected from CSPs and participating CI entities is limited to that which is necessary to coordinate activities under the program and share threat information. There is very little privacy risk associated with the amount or character of information collected about program participants.

Thus, DHS only collects a modest amount of contact information from the submitter and additional PII only if it is, itself, a threat indicator. The privacy risks of this collection are greatly reduced by the deliberate failure to link any PII that is part of a threat indicator to the individual it purports to be about. As noted above, in many cases, is it impossible to create such links.

There are few risks associated with this principle through the established sharing practices. DHS will not share PII routinely collected from participants. Moreover, despite the fact that threat indicators are not linked to an individual (a fact that is understood by the limited number of recipients), CS&C SOPs further require a review of the proposed dissemination, under which all PII will be overwritten, redacted, or replaced, unless it is necessary for recipients to understand the threat.

Use Limitation:

Use of both contact information collected from ECS participants and that related to threat indicators is limited to the narrow purposes of the ECS program.

The MOA between DHS and participating CSPs explicitly limits CSPs' use of data to the purposes outlined in the agreement, purposes that align with ECS authorities. Other uses are not permitted. Moreover, the MOA limits access within the CSP's organization to individuals who have the appropriate security clearance and who have a need to know the information in accordance with a set of security guidelines that have been reviewed in advance by CS&C.

Data Quality and Integrity:

The data quality and integrity of information collected by DHS about program participants is related to the program's implementation of a number of the other FIPPs. First, contact information—including PII—is received directly from the program participants, which is a significant indicator of data quality. Second, since the purpose of this data collection is limited to that which is necessary to facilitate (1) the suitability of participation for CSPs and CI entities, and (2) the effective sharing of threat information, program participants may contact the ECS Program Office at any time to update or correct inaccurate or erroneous information.

For threat indicators, the government's interest is in effectively conveying accurate threat information to program participants. Therefore, mission drivers will enhance accuracy of any PII in the threat reporting. Even if errors occur, however, since there is no link in this information to an individual, there will be minimal impact on privacy. Finally, in support of data integrity, the ECS MOA requires recipients to maintain facilities capable of receiving, sending, and storing classified information. These protections substantially reduce the likelihood of loss of control of data, or unauthorized access or corruption of program data, including PII.

Security:

As many threat reports, including threat indicators, are protected with national security classifications as high as Top Secret/Sensitive Compartmented Information, information use and handling requirements are driven by national security laws that are designed to ensure effective security procedures are in place and maintained by all parties who access threat reports.

The MOA between DHS and CSPs contains a number of provisions related to security. These include requirements that: (1) CSPs abide by written Security Guidelines issued by DHS; (2) CSPs maintain an accredited facility to receive and store classified information; and (3) DHS perform an assessment of CSPs' security network design and environments for information received from the government under this program.

These provisions greatly reduce the likelihood that security gaps will expose cyber threat information (and any PII contained in it) shared under the ECS to unauthorized users.

Accountability and Auditing:

CSPs are responsible for the duties outlined for them in the MOA they must sign to participate in the ECS program. Failure to abide by the terms and conditions of the MOA is grounds for termination, the only remedy available. Once a decision to terminate is made, the CSP leaving the program is required to permanently destroy or return any information it received from the government, including PII.

CSPs' ability to continue receiving classified information over time is conditioned on their continuing to meet the requirements that their personnel hold security clearances and that they maintain facilities to receive and store classified information. These requirements include periodic background investigations for personnel, and granting access to DHS-approved security personnel to verify proper installation, logical configuration, and operation for security purposes for the protection of classified information within CSP facilities. Personnel who fail to follow clearance requirements can be criminally prosecuted.

Finally, the participating CSPs may report cybersecurity metrics that will help the government understand the ongoing value of the ECS program. As mentioned above, these metrics focus on aggregated information about the character and scope of an attack, rather than on details about the attack's targets. These metrics help program participants periodically reassess the value of continuing in the voluntary ECS program, in light of their own perceived privacy risks.

Legal Considerations Relevant to Civil Liberties

CRCL worked with the DHS Office of General Counsel to examine the legal basis of the ECS program. CRCL is satisfied that the program meets applicable legal requirements and that the program's legal compliance efforts appropriately protect individual rights. The legal analysis is not included in this report because it is subject to deliberative and attorney-client privileges.

Civil Liberties Policy Considerations

The primary civil liberties concerns with ECS revolve around whether the government is using the system to monitor and/or unreasonably collect private sector or other non-federal internet communications, either directly or by using the CSPs as a proxy to perform the collection. Some have also voiced more specific concerns that this program could be used to conduct targeted monitoring of individuals, either for criminal investigative or intelligence surveillance purposes. These concerns are not trivial. Most signature-based cybersecurity technologies involve some monitoring of electronic communications, and any presence of the U.S. Government in close proximity to communications enterprises is likely to raise those questions. These questions may revolve around the Government's role, its actions and intent, whether it is in compliance with all applicable laws, and whether there are appropriate policies in place to safeguard individual rights. CRCL assesses that the ECS Program, as it is presently structured, does not involve the government monitoring or collecting communications content or metadata, nor does it involve the government using the CSPs or their CI entity clients to perform such monitoring or collection on its behalf. CRCL has also determined that the program's policies establish a suitable

compliance framework, providing appropriate protections of individual rights commensurate with program activities and its current stage of development.

As explained above in the "How ECS Functions" section, the written agreements governing the relationship between DHS and the CSPs[27] pertain only to information sharing, specifying the types of information to be shared, and how the information will be safeguarded. Other than setting security requirements with which CSPs must comply, these agreements do not permit the government to control the activities of the CSPs.

In an outward-bound direction, only threat information and safeguarding requirements are included in the GFI. For example, DHS may provide information about a particular cyber threat, but it cannot direct a CSP to monitor communications on behalf of a particular CI entity that may be a target of that threat, nor can it attempt to use this process to establish the equivalent of a wiretap targeting prospective adversaries. Concordantly, the CSPs have not agreed to collect any communicative content or metadata beyond the "fact of" metrics described above, and there is no provision allowing the government to require the CSPs to collect additional data from the CI entities. Even the provision of "fact of" data is voluntary, and it is up to the CSP and their CI entity client to determine whether they wish to provide that feedback.

While CSPs may inform DHS when they have encountered a threat corresponding to GFI and the CI sector in which that threat was encountered, the information to be provided to DHS is stripped of PII, anonymized, and provided in an aggregated or collected format. It will not contain the communications content of the individuals whose communications were monitored by the CSP, name the affected CI entity, nor contain any metadata about the compromised communication. The information collected is to be used primarily as a metric, to determine the effectiveness of ECS and of the specific pieces of threat information shared. If the CI entity or the CSP does not wish to provide this information, it does not have to do so. Any additional information a CI chooses, of its own volition, to report, will not be handled through ECS but will be referred to other appropriate DHS or partner agency offices.[28] In their MOA with DHS, CSPs agree not to provide any information derived from their provision of ECS services other than the aggregated, anonymized, fact-of metrics called out in the MOA. The provision of any further information is prohibited by the MOA.

The information sharing is not unconditional; it does have some "strings" attached, but they do not amount to a government exercise of control over CSPs' monitoring activity or government access to CI entities' data. Instead, they are preconditions aimed at safeguarding the GFI that will be shared with the CSPs. Before sharing any GFI, DHS articulates security safeguarding standards that CSPs are required to adopt as a condition of participation. This entails the construction or identification of facilities capable of properly securing the GFI. Within ECS operations, a limited amount of the GFI furnished to the CSPs is provided on the condition that if

[27] The written agreements (MOA) governing the DHS-CSP relationship do not include or extend to the CI entities; once an entity is validated as being an owner or operator of CI, DHS has no further role and the Department is not involved at any point in the relationship between the CI entity and the CSP it chooses.

[28] This policy keeps ECS tightly focused on information sharing as described in this document, while ensuring that participation in ECS does not preclude a CI from seeking additional government cybersecurity assistance through channels other than the ECS program should it choose to do so.

the CSP chooses to employ that particular threat information, it may do so only in conjunction with a particular countermeasure. Such a precondition does control CSP activities generally, but ensures that if a CSP chooses to employ GFI obtained by sensitive sources and methods, the countermeasure employed does not alert the adversary and result in the compromise of those sensitive sources and methods.

Also ensuring the voluntariness of this program is the nature of the CSPs involved. The providers will generally be large, sophisticated ISPs, cybersecurity firms, or other firms with significant inherent capabilities that give them the ability to identify and respond to sophisticated technical threats, to handle sensitive GFI appropriately, and to provide technically complex protective capabilities for themselves or clients. They enter the program voluntarily, they may leave it at any time, and there is no sanction attached to a CSP's choice not to employ a particular piece of GFI or to leave the program. The voluntariness extends to the CSPs' choice of validated CI clients, to their duration of participation, and even to which threat indicators the CSPs choose to rely upon in their cybersecurity activities. The CI entities have similar latitude.[29] They are not participating by virtue of government compulsion; they have their own incentives to seek cybersecurity services, and the services they obtain through an ECS participant CSP resemble the types of cybersecurity services they are likely to be seeking, or receiving already. The addition of GFI offers something they presently lack.

On balance, the relationship between the U.S. Government and the CSPs is best viewed as a voluntary information sharing partnership, with most of the sharing involving the sharing of GFI with CSPs, and with little information shared in return with the Government. The government does not exercise control over the CSPs' or CI entities' activities, it does not direct them, and it does not contemplate using this relationship as a method of circumventing restrictions on other types of collection and investigative activities. We assess that the current impact on civil liberties from this process is minimal.

Recommendations:

6. The Privacy Office recommends that the Department continue its vigilant oversight of the ECS program, in order to ensure that, should privacy impacts arise, they are identified and addressed promptly. To that end, the Privacy Office intends to conduct an in-depth Privacy Compliance Review of the entire ECS Program in 2014, and will report the results in the 2015 annual report required by EO 13636.

CRCL believes that the ECS Program, as currently structured, has little to no effect on the civil liberties of individuals and that additional modifications to the program and protections are not needed at this time. Ongoing vigilance is necessary due to the ever-present threat of mission-creep, and because as programs evolve and grow, new and frequently unanticipated civil liberties concerns may arise. The Department and the ECS Program will need to continue to build in policies that protect individual rights as the program matures and grows larger. CRCL plans to

[29] The relationship between the protected CI entities and the CSPs does not factor into this evaluation, because after an entity is validated as being a CI entity, that entity's choice of CSP (if it chooses one) and the nature and extent of services it obtains from the CSP is strictly between that CI entity and the CSP.

continue working closely with the ECS Program office on an advisory basis, and will conduct further assessments or oversight activity as appropriate.

IV. EO Implementation Activity: The DHS Private Sector Clearance Program

EO Section 4(d):

> *The Secretary, as the Executive Agent for the Classified National Security Information Program created under Executive Order 13549 of August 18, 2010 (Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities), shall expedite the processing of security clearances to appropriate personnel employed by critical infrastructure owners and operators, prioritizing the critical infrastructure identified in section 9 of this order.*

Program Description

The Department is building upon NPPD's Critical Infrastructure Private Sector Clearance Program (PSCP) to implement Section 4(d) of EO 13636. The PSCP is administered by the Office of Infrastructure Protection (NPPD/IP) and the DHS Office of the Chief Security Officer (OCSO) Personnel Security Division.

Through the PSCP, NPPD/IP sponsors security clearances for CI owners and operators, and other subject matter experts, to assist in analyzing CI-related national security information to enhance the Department's infrastructure protection mission. The PSCP also ensures that CI private sector owners, operators, and industry representatives, specifically those in positions with responsibilities for ensuring the protection, security, and resilience of CI, have access to information to make informed decisions. Established in 2006, the PSCP has sponsored more than 1,680 private sector individuals for security clearances. NPPD/IP has implemented enhancements to the PSCP to meet the intent of EO 13636, including a new process for prioritizing clearance applications (including applications from cybersecurity experts), and enhanced reporting to SSA, and entities identified under Section 9 of the EO, on clearance holders and the status of clearance applications.

As discussed more fully below, clearance processing in PSCP proceeds in three phases: (1) applicant processing; (2) investigation; and (3) adjudication. In Phase 1, PSCP initiates the application process by working with Nominators (i.e., federal officials designated by NPPD/IP) to identify prospective participants and by reviewing initial applications, which include certain PII. PSCP then routes the application to the NPPD/IP Office of the Assistant Secretary for review. If the application is approved, the IP Security Office collects additional PII and initiates the background investigation process administered electronically by the U.S. Office of Personnel Management (OPM).

OPM and the DHS OCSO Personnel Security Division conduct the background investigation required to obtain a security clearance and the adjudication of the clearance, respectively. During Phases Two and Three, OPM or the Personnel Security Division may require additional PII from applicants. This additional information is neither shared with PSCP nor stored in the PSCP system. PSCP collects and retains only that information necessary to monitor the status of an individual's clearance processing. The Personnel Security Division notifies PSCP of the

results of the adjudication of the clearance. In the event of a denial, PCSP retains only the applicant's name, CI sector, and date of denial.

ITF Working Group

As the task required by EO Sections 4(d) entailed further development of an existing DHS program, there was no need to assign an ITF Working Group to accomplish it.

Deliverable

DHS Memorandum from then-DHS Secretary Janet Napolitano to Lisa Monaco, Assistant to the President for Homeland Security and Counterterrorism, entitled "Progress on Executive Order 13636 Requirement 4(d) - Expediting the Processes for Security Clearances," (July 12, 2013), transmitting a *Private Sector Clearance Program Overview*.

Additional Resources

A PSCP Fact Sheet will be posted on the DHS website later this year.

Privacy and Civil Liberties Risks/Impacts of the PSCP

Privacy Compliance Documentation

The DHS Privacy Office and the NPPD Office of Privacy collaborated to conduct and publish a PIA for the PSCP on November 2, 2011.[30] The PIA discusses the potential privacy impacts of the Program and the steps taken to mitigate them. The SORN applicable to the collection of information in the PSCP is *DHS/ALL–023 Department of Homeland Security Personnel Security Management*, which was updated most recently in February 2010.[31]

FIPPs Analysis

Transparency:

The PIA for PSCP includes a full description of the Program and describes how potential privacy risks have been mitigated by implementing the FIPPs. The PIA is available on the DHS Privacy Office website.

[30] The PSCP PIA, DHS/NPPD/PIA-020 is available on the DHS Privacy Office's website at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_nppd_pscp.pdf.
[31] The SORN is available at www.gpo.gov/fdsys/pkg/FR-2010-02-23/html/2010-3362.htm.

Information collected in PSCP, and the additional information collected by the Personnel Security Division, is covered under the SORN entitled DHS/ALL–023 Department of Homeland Security Personnel Security Management, 75 FR 8088 (February 23, 2010), which provides further transparency into the information collection process required for obtaining security clearances.

In addition, the PSCP provides direct notice to individual applicants explaining how their information will be used by the Program and why that information is needed. This is accomplished by means of a Privacy Act subsection (e)(3) Statement[32] included on the initial PSCP application form, DHS Form 9014, *Critical Infrastructure Privacy Sector Clearance Program Request*.

Individual Participation:

Participation in the PSCP is entirely voluntary. Information about participants, including all PII, is supplied by the participants themselves. Individuals can opt out of the Program at any time by notifying the Nominator or PSCP Administrator of their intent to do so. If an individual chooses to opt out of the Program after having begun or completed the clearance process, his or her records will be removed from the Program roster and associated hard copy records moved to a separate file that is purged after three years.[33]

Purpose Specification:

PSCP is being conducted pursuant to authority derived from Section 201 of the Homeland Security Act, 6 U.S.C. § 121, and EOs 9397,[34] 12968,[35] 13526,[36] and 13549.[37] There is no risk to privacy associated with the authorities supporting the PSCP. Both the PIA for PSCP and the

[32] Privacy Act (e)(3) statements are required by the Privacy Act to appear on government forms that collect PII and are part of formal notice providing transparency to the person about whom the information is being collected. 5 U.S.C. § 552a(e)(3).
[33] The PSCP PIA provides more information on records retention under the PSCP.
[34] Executive Order 9397, as amended, gives agencies the authority to collect Social Security numbers whenever they find it advisable to set up a new identification system for individuals. EO 9397, *Numbering System for Federal Accounts Relating to Individual Persons*, 8 FR 16095 (November 30, 1943), as amended by EO 13478, *Amendments to Executive Order 9397 Relating to Federal Agency Use of Social Security Numbers*, 73 FR 70239 (November 20, 2008).
[35] Executive Order 12968 establishes a uniform federal personnel security program for employees who will be considered for initial or continued access to classified information. It requires that individuals who are granted access to classified information are subject to continuous evaluation according to standards determined by the Director of National Intelligence. EO 12968, *Access to Classified Information*, as amended by EO 13467, *Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information*, 73 FR 38103 (July 2, 2008).
[36] Executive Order 13526 prescribes a uniform system for classifying, safeguarding, and declassifying national security information, including information relating to defense against transnational terrorism. EO 13526, *Classified National Security Information*, 75 FR 705 (January 5, 2011).
[37] Executive Order 13549 establishes a Classified National Security Information Program designed to safeguard and govern access to classified national security information shared by the Federal Government with state, local, tribal, and private sector entities. EO 13549, *Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities*, 75 FR 51615 (August 23, 2010).

applicable SORN specify the purposes for which the PSCP collects PII and the uses of that information.

Data Minimization:

To minimize the collection of PII, PSCP collects information in two separate steps. Applicants provide the following PII on DHS Form 9014 with their initial applications: full name; company name; business title; business physical and email addresses and phone number; business relationship to the relevant CI sector; and the applicant's citizenship. If the IP Office of the Assistant Secretary approves the initial application, then the IP Security Office contacts the applicant directly to obtain the applicant's date and place of birth and Social Security number (SSN) and enters the applicant's name, date and place of birth, SSN, and business email address into OPM's secure portal for investigation processing, the Electronic Questionnaire for Investigation Process (e-QIP).[38] The applicant then accesses e-QIP directly to complete and submit OPM's electronic security questionnaire, Standard Form 86, *Questionnaire for National Security Positions.* PSCP neither collects nor has access to the personal information that the applicant provides to OPM.

Use Limitation:

PSCP's use of PII collected from PSCP participants is limited to the narrow purposes of the PSCP program. The Program shares limited information with OPM, as noted above, in order to initiate an applicant's submission of personal information into Standard Form 86 through e-QIP.

PSCP is now sending SSAs monthly reports listing all clearance applications and clearance holders in their respective CI sectors. These reports are transmitted securely, and the PII in them is limited to individuals' names, organization information, and application status.

In addition, PSCP may at times share lists of cleared individuals with federal agencies other than DHS to facilitate clearing those individuals for participation in classified communications hosted by those agencies. The Program would accomplish this by extracting relevant information from its clearance roster, sanitizing the list to remove any Sensitive PII, and sharing information pertaining only to those participants who require access to the classified briefing. The sanitized list would include only a participant's full name, company name, city and state, and business email address. PSCP does not share any Sensitive PII outside of DHS.[39] This sharing is compatible with the routine uses published in the DHS Personnel Security Management SORN.[40] If PSCP shares any participant's information with an external agency, the information is marked as For Official Use Only Privacy Act Information, and the recipient is notified not to further disseminate it.

[38] For more information on e-QIP, see OPM/CENTRAL-9 - Personnel Investigation Records, 75 FR 28307 (May 20, 2010).
[39] If Sensitive PII were required by an outside agency to verify and individual's security clearance, the Personnel Security Division, and not PSCP, would send that information to the external agency.
[40] 75 FR 8088 (February 23, 2010).

Data Quality and Integrity:

PSCP receives all PII directly from the Program applicants and participants, which is a significant indicator of data quality. As the purpose of this data collection is limited to that which is necessary to facilitate the granting of security clearances, both the applicant and DHS have every reason to take all reasonable steps to identify and correct errors in the data necessary to support this purpose. Once OPM initiates a background investigation, OPM works directly with applicants and provides them an opportunity to correct inaccurate or erroneous information. These protections substantially reduce the likelihood that adjudication of requests for security clearances would be based on outdated or otherwise inaccurate information.

Security:

A PSCP applicant's printed e-QIP signature pages, but not the content of the completed Standard Form 86, are part of a package of DHS forms and standard security forms that applicants must submit before the investigation process begins. The forms package also includes a set of fingerprint cards and a DHS Form 11000-9, *Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act*. The Program instructs applicants to submit two copies of this package, one in hard copy and one in electronic form. The Program retains the hard copy in the individual's file in a locked filing cabinet, and the electronic copy is password-protected and stored on the Program's access-restricted shared drive. The NPPD/IP Security Office sends the complete, electronic package of forms, fingerprints, including the DHS Form 9014, *Critical Infrastructure Private Sector Clearance Program Request*, to the Personnel Security Division, via a password-protected email attachment, for processing.

These processes, together with the electronic process for submitting information to OPM on Standard Form 86, greatly reduce the risk that PSCP applicants' PII would be lost, exposed to unauthorized users, or used for an unauthorized purpose.

Accountability and Auditing:

Only the NPPD/IP Security Office staff directly supporting the Program have access to the PSCP's physical and electronic files. Strict access controls are in place to ensure that only those with an authorized purpose and need to know have access to PSCP data. All PSCP employees and contractors receive the annual privacy training required of all DHS personnel.

The DHS OCSO Administrative Security Division and the DHS Office of Inspector General also conducted reviews of the Program. The NPPD Office of Privacy and the DHS Privacy Office regularly coordinate with the PSCP to ensure that PII obtained in the PSCP is used in accordance with the practices and procedures described in the PSCP PIA. In November 2013, the NPPD Office of Privacy completed a mandatory PTA for PSCP to review changes in the Program since the PIA was published, including the enhanced reporting implemented pursuant to EO 13636. The review identified no new privacy risks that would merit the updating of the PIA.

Civil Liberties Policy Considerations

The Office for Civil Rights and Civil Liberties reviewed this activity, its standards and the criteria for participation in it, and found no significant civil rights or civil liberties issues requiring discussion and assessment at this time.

Recommendations

As noted above, the NPPD Office of Privacy's November 2013 assessment of the PSCP found that no additional privacy risks are posed by the enhancements NPPD has implemented pursuant to EO 13636. The DHS Privacy Office concurs in that assessment and, therefore, proposes no additional privacy protections at this time. Together with the NPPD Office of Privacy, the DHS Privacy Office will continue to monitor PSCP to ensure that the Program continues to implement the privacy protections currently in place. Should additional changes take place in the Program that affect privacy, the DHS Privacy Office will assess the risks posed and the steps taken to mitigate them, and will include its assessment in future EO 13636 Privacy and Civil Liberties Assessment Reports.

V. EO Implementation Activity: The DHS Loaned Executive Program

EO Section 4(e):

> *In order to maximize the utility of cyber threat information sharing with the private sector, the Secretary shall expand the use of programs that bring private sector subject-matter experts into Federal service on a temporary basis. These subject matter experts should provide advice regarding the content, structure, and types of information most useful to critical infrastructure owners and operators in reducing and mitigating cyber risks.*

As a complement to the PSCP, the Department is leveraging its existing Loaned Executive Program to implement Section 4(e) of EO 13636. DHS established the Loaned Executive Program in 2008. The Program, which is administered by the DHS Private Sector Office, provides an unpaid opportunity for executive-level experts from the private sector to share their expertise with DHS. As determined by DHS components hosting them, participants are assigned to serve as subject matter experts or senior advisors to DHS leadership, evaluate existing policies, procedures, and training, and/or provide guidance on the public-private partnership model and implementation of strategies designed to improve private sector engagement with DHS. Prospective participants undergo the Office of Security Personnel Security Division's process for obtaining security clearances through the PSCP.[41]

The Department is currently expanding the Loaned Executive Program to include private sector cybersecurity experts by developing focused cybersecurity-related assignments for prospective participants. The DHS Privacy Office will work with the Private Sector Office to conduct a PIA for the Program, to identify and mitigate any privacy risks not addressed in an existing PIA. The DHS Privacy Office will provide a detailed assessment of the expanded Loaned Executive Program in the 2015 EO 13636 Privacy and Civil Liberties Assessment Report.

Civil Liberties Policy Considerations

The Office for Civil Rights and Civil Liberties reviewed this activity, its standards and the criteria for participation in it, and found no significant civil rights or civil liberties issues requiring discussion and assessment at this time.

Recommendation

7. The DHS Privacy Office recommends that cybersecurity experts in the Loaned Executive Program receive appropriate privacy training as a condition of participation in the Program. The Privacy Office will provide guidance and assistance to the Program to support development of the privacy training.

[41] More information on the Loaned Executive Program is available on the DHS website at http://www.dhs.gov/loaned-executive-program.

Appendix 1: Acronym List

CI	Critical Infrastructure
CRCL	Office of Civil Rights and Civil Liberties
CS&C	Office of Cybersecurity & Communications
CSP	Commercial Service Provider
DHS	U.S. Department of Homeland Security
DOJ	U.S. Department of Justice
DPIAC	Data Privacy and Integrity Advisory Committee
E^3A	EINSTEIN 3 Accelerated
ECS	Enhanced Cybersecurity Services
EO	Executive Order
e-QIP	Electronic Questionnaire for Investigation Process
FIPPs	Fair Information Practice Principles
GFI	Government Furnished Information
I&A	Office of Intelligence and Analysis
ICD	Intelligence Community Directive
ISP	Internet Service Provider
ISWG	Information Sharing Working Group
ITF	Integrated Task Force
MOA	Memorandum of Agreement
NCCIC	National Cybersecurity and Communications Integration Center
NCPS	National Cybersecurity Protection System
NPPD	National Protection and Programs Directorate
NPPD/IP	Office of Infrastructure Protection
OCSO	Office of the Chief Security Officer
ODNI	Office of the Director of National Intelligence
OI	Operational Implementer
OPM	U.S. Office of Personnel Management
PCII	Protected Critical Infrastructure Information
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PPD-21	Presidential Policy Directive 21
PSCP	Private Sector Clearance Program
PTA	Privacy Threshold Analysis
SOP	Standard Operating Procedure
SORN	System of Records Notice
SSA	Sector Specific Agency
SSN	Social Security Number
US-CERT	United States-Computer Emergency Readiness Team

PART II

DEPARTMENT OF THE TREASURY

DEPARTMENT OF THE TREASURY
WASHINGTON

ASSISTANT SECRETARY

DEC 12 2013

Megan H. Mac
Officer for Civil Rights and Civil Liberties
Department of Homeland Security

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security

Transmittal: Department of the Treasury Privacy and Civil Liberties Assessment

In accordance with Section 5(b) of Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, attached please find an assessment of the Department of the Treasury's activities under the Executive Order.

Sincerely,

Nani Coloretti
Assistant Secretary for Management
(Senior Agency Official for Privacy/
Privacy and Civil Liberties Officer)

Attachment

DEPARTMENT OF THE TREASURY
ASSESSMENT OF THE IMPLEMENTATION OF EO 13636
IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY

INTRODUCTION:

On February 12, 2013, the President signed Executive Order ("E.O." or "Order") 13636, *Improving Critical Infrastructure Cybersecurity*, stating: "It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber-environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties."

Section 5(a) of the EO requires federal agencies to coordinate EO-related cybersecurity activities with their senior agency officials for privacy and civil liberties (SAOP), to conduct an assessment of agency activities under the EO, and to submit the assessment to the Department of Homeland Security (DHS) for consideration and inclusion in the DHS public report, due within one year of the date of the issuance of the EO.

The Department of the Treasury (Treasury) submits the following assessment of Treasury activities under the EO.

Section 4: Cybersecurity Information Sharing.

> *(a) It is the policy of the United States Government to increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities so that these entities may better protect and defend themselves against cyber threats.*
>
> *(d) The [DHS] Secretary, as the Executive Agent for the Classified National Security Information Program created under Executive Order 13549 of August 18, 2010 (Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities), shall expedite the processing of security clearances to appropriate personnel employed by critical infrastructure owners and operators, prioritizing the critical infrastructure identified in section 9 of this order.*

As the Sector Specific Agency (SSA) for the Financial Services Sector, Treasury serves as the primary point of contact for individuals in the sector who require security clearances. To facilitate the identification and processing of security clearances for appropriate sector personnel, Treasury participates in the DHS Critical Infrastructure Private Sector Clearance Program.

Treasury uses DHS Form 9014 "Critical Infrastructure Private Sector Clearance Program Request"[1] to collect the following information:

- Name

[1] OMB No. 1670-0013

- Company Name/Address
- Phone Number
- E-mail address
- Level of Clearance
- Citizenship

Once collected, Treasury sends the partially completed DHS Form 9014s (date and place of birth and Social Security numbers are not collected by Treasury) to the DHS Critical Infrastructure Private Sector Clearance Program Office. DHS contacts individuals directly to collect additional information as necessary to begin the investigative process for a security clearance. To help track the status of clearances, Treasury regularly receives updates from DHS in the form of a clearance roster.

Assessment:

At no time does Treasury request, receive, or retain sensitive information (e.g., Social Security number, date of birth). Information collected from the public and received from DHS is stored in a secured folder on the shared drive, with access limited to only those who have a need to know. Records are maintained from the time an applicant begins the clearance application process until their security clearance is deactivated or the individual's participation with the Program is terminated. The records retention schedule is covered by the NARA General Records Schedule (GRS) 18 Items 21; 22; 23.

Section 8. Voluntary Critical Infrastructure Cybersecurity Program.

> *(a) The Secretary [DHS], in coordination with Sector-Specific Agencies, shall establish a voluntary program to support the adoption of the Cybersecurity Framework by owners and operators of critical infrastructure and any other interested entities (the ''Program'').*
>
> *(d) The Secretary shall coordinate establishment of a set of incentives designed to promote participation in the Program. Within 120 days of the date of this order, the Secretary and the Secretaries of the Treasury and Commerce each shall make recommendations separately to the President, through the Assistant to the President for Homeland Security and Counterterrorism and the Assistant to the President for Economic Affairs, that shall include analysis of the benefits and relative effectiveness of such incentives, and whether the incentives would require legislation or can be provided under existing law and authorities to participants in the Program.*

Pursuant to the requirement, Treasury submitted recommendations to the President,[2] including an analysis of the benefits and relative effectiveness of incentives designed to promote participation in the Voluntary Critical Infrastructure Cybersecurity Program. Proposed incentives include the timely release of pertinent cybersecurity information, recommendations

[2] Treasury Department Report to the President on Cybersecurity Incentives Pursuant to Executive Order 13636: http://www.treasury.gov/press-center/Documents/Supporting%20Analysis%20Treasury%20Report%20to%20the%20President%20on%20Cybersecurity%20Incentives_FINAL.pdf

for expediting the security clearance process for appropriate critical infrastructure employees, establishing clear cybersecurity standards, an insurance model, increasing government grants for cybersecurity research and development, and tax incentives for targeted cybersecurity investments.

Assessment:

Treasury's recommendations for increasing participation primarily focus on government incentives to address market failures (i.e., funding research and development in areas that may not be to a private organization's net benefit) and do not pose a risk to individual privacy and civil liberties. Recommendations outside the use of market mechanisms focus on improved access to cybersecurity information through expedited security clearances and increased dissemination of information from the government to the private sector. Improved information sharing, and resulting actions, could potentially pose a risk to individual privacy and/or civil liberties if personal information (e.g., personal e-mail address, business contact information, IP address) is associated with a cyber-threat. The supporting analysis in Treasury's recommendations notes that certain protocols, such as removing any personally identifiable elements that are not relevant to cybersecurity, help avoid compromising individual privacy and civil liberties. While Treasury has the authority to increase its dissemination of timely cyber threat information to the financial services sector, any dissemination must be consistent with applicable authorities including laws protecting privacy, civil liberties, and national security information.

Section 9. Identification of Critical Infrastructure at Greatest Risk.

> *(a) Within 150 days of the date of this order, the Secretary shall use a risk-based approach to identify critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security. In identifying critical infrastructure for this purpose, the Secretary shall use the consultative process established in section 6 of this order and draw upon the expertise of Sector-Specific Agencies.*
>
> *(b) Heads of Sector-Specific Agencies and other relevant agencies shall provide the Secretary with information necessary to carry out the responsibilities under this section.*
>
> *(c) The Secretary, in coordination with Sector-Specific Agencies, shall confidentially notify owners and operators of critical infrastructure identified under subsection (a) of this section that they have been so identified, and ensure identified owners and operators are provided the basis for the determination.*

Treasury consulted with DHS on the process for identifying critical infrastructure in which a cybersecurity incident could reasonably result in catastrophic consequences. Treasury is in the process of identifying appropriate points of contact (POCs) for critical infrastructure identified under this section.

Assessment:

Information collected about owners and operators of identified infrastructure is limited to business contact information and is stored in a secured folder on a secure computer network with access limited to only those that have a need to know. Pursuant to the EO, the POCs will be contacted directly and confidentially notified that DHS has identified their respective entity as cyber-dependent critical infrastructure under Section 9.

PART III

DEPARTMENT OF DEFENSE

DEPARTMENT OF DEFENSE
DEFENSE PRIVACY AND CIVIL LIBERTIES OFFICE
241 18TH STREET SOUTH, SUITE 101
ARLINGTON, VA 22202

Megan H. Mack
Officer for Civil Rights and Civil Liberties
US Department of Homeland Security
Washington, DC 20528-0655

DEC 13 2013

Via electronic submission

Dear Ms. Mack:

Pursuant to section 5(b) of Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," this letter and its enclosures serve as the Department of Defense's privacy and civil liberties assessment of agency activities for DHS consideration.

Samuel P. Jenkins
Acting Director

Enclosures:
As stated

DEPARTMENT OF DEFENSE
DEFENSE PRIVACY AND CIVIL LIBERTIES OFFICE
241 18TH STREET SOUTH, SUITE 101
ARLINGTON, VA 22202

Karen Neuman
Chief Privacy Officer
US Department of Homeland Security
Washington, DC 20528-0655

DEC 13 2013

Via electronic submission

Dear Ms. Neuman:

Pursuant to section 5(b) of Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," this letter and its enclosures serve as the Department of Defense's privacy and civil liberties assessment of agency activities for DHS consideration.

Samuel P. Jenkins
Acting Director

Enclosures:
As stated

Department of Defense

Executive Order 13636, "Improving Critical Infrastructure Cyber Security," Section 5 Assessment of Privacy and Civil Liberties Protections

Executive Order 13636, Section 5

Executive Order 13636 established U.S. policy to increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities. Section 5 requires senior agency officials for privacy and civil liberties to incorporate privacy and civil liberties protections into such activities, and to conduct assessments of those activities, based upon the eight Fair Information Practice Principles (FIPPs) and other applicable policies, principles, and frameworks.

Defense Industrial Base (DIB)[1]

DIB is the Department of Defense (DoD), U.S. government, and private-sector worldwide industrial complex with capabilities to perform research and development, design, produce, deliver, and maintain military weapon systems, subsystems, components, or parts to meet military requirements. The DIB includes hundreds of thousands of domestic and foreign entities and their subcontractors performing work for DoD and other Federal agencies. Defense-related products and services provided by the DIB equip, inform, mobilize, deploy, and sustain forces conducting military operations.

DoD is the U.S. Sector-Specific Agency (SSA) for the DIB. As such, DoD is required to:

- Collaborate with all relevant Federal departments and agencies, state and local governments, and the private sector, including with key persons and entities in the DIB sector;
- Conduct or facilitate vulnerability assessments of the DIB sector; and
- Encourage risk management strategies to protect against and mitigate the effects of attacks against critical infrastructure and key resources.

To execute its responsibilities for the DIB successfully, DoD must engage in ongoing activities to build trust with DIB critical asset owners and operators to support two-way information sharing and to maintain meaningful relationships and frequent dialogue across the diverse array of DIB stakeholders. Private-sector critical infrastructure program participation is voluntary.

---

[1] *See generally,* http://policy.defense.gov/OUSDPOffices/ASDforHomelandDefenseAmericasSecurityAffa/DefenseCriticalInfrastructureProgram/Partnering.aspx

Many large size defense industry firms place a great deal of emphasis on protecting their physical, human, and cyber assets. On the other hand, many of the medium and smaller size businesses are challenged to make the capital investments required to perform vulnerability assessments and build resiliency into their operational capabilities.

DIB Cyber Security/Information Assurance (CS/IA) Program

DIB CS/IA Program is designed to improve DIB network defenses and allows DIB companies and the government to reduce damage to critical programs when defense information is compromised. The DIB CS/IA Program includes a voluntary information sharing component under which DIB companies and the government agrees to share cyber security information out of a mutual concern for the protection of sensitive, but unclassified information, related to DoD programs on DIB company networks. The DIB CS/IA Program is open to all eligible DIB companies. Currently, there are nearly 100 companies participating in the program.

Under the DIB CS/IA Program, DoD provides participating DIB companies with unclassified cyber threat indicators and related classified contextual information. DIB companies can choose whether to incorporate the indicators into their own traffic screening or other security tools and use the contextual information to better understand the cyber security threats they face. DoD also shares mitigation measures to assist DIB companies' cyber security efforts.
DIB companies also report known intrusion events that may have affected DoD information to DoD and may participate in DoD damage assessments, if needed. Participating DIB companies agree to report any cyber incidents they discover on their networks that have resulted in an actual or potential compromise of DoD information, and may also, at its discretion, report any other cyber event that may be of interest to the government and the DIB cyber community. The electronic media provided by the participating DIB company is analyzed in support of cyber intrusion damage assessments to determine the impact of compromises on DoD programs.

DIB CS/IA Program and Personally Identifiable Information

The DIB CS/IA Program seeks to minimize the collection and management of personally identifiable information (PII), except when necessary to support the program There are two types of PII involved with the program: (1) DIB company Point of Contact (POC) PII and (2) inadvertent PII collected as a result of electronic transmission or other data collected responding to a cyber-incident, including analysis.

- **POC PII for program administration and management purposes**. DIB companies share with DoD typical business contact information for its personnel that are serving as company POCs for DIB CS/IA Program activities or specific cyber incidents. This PII is limited to the individual's contact information that is routinely shared in the ordinary course of business (e.g., name, title, organizational division, business email and phone number), along with

other information (e.g., security clearance, citizenship) that is necessary to verify the individual's authorization to receive classified or other controlled unclassified information under the program. This information is covered by the Privacy Act Statement (PAS), the program's System of Records Notice[2] (SORN), and Privacy Impact Assessment[3] (PIA).

- **Inadvertent PII for cyber incident response and analysis purposes**. Although it is not typical or expected, there exists the potential that information provided by a DIB company regarding a specific cyber incident may include PII that is incidental to, or embedded in, the information being shared for cyber security analysis.[4] This information is shared with DoD only if the DIB company determines that the PII is relevant to the incident response and analysis, and that there are no legal, contractual, or other restriction on sharing the PII with the U.S. government. This PII is detailed in the program's PIA, not in the DIB CS/IA Program SORN or PAS.[5]

DIB Enhanced Cyber Security Services (DECS)

DECS is an optional component of the DIB CS/IA Program and is conducted by DoD in coordination with the Department of Homeland Security (DHS). Under DECS, DHS is the government point of contact for commercial service providers (CSPs).[6] The government will furnish threat information to DHS approved CSPs. This includes information assurance data such as internet protocol addresses. CSPs use that information and offer specified services to DIB customers in a secure environment designed to ensure the security of sensitive government furnished information, while countering malicious cyber activity and protecting DoD program information. CSPs deliver the DECS services to eligible DIB customers through commercial relationships.

A DIB company may elect to participate in DECS in several different ways: by purchasing the services from a participating DHS-approved CSP, by meeting the security requirements to

---

[2] *See* SORN at http://dpclo.defense.gov/privacy/SORNs/component/osd/DCIO_01.html
[3] *See* PIA at http://dodcio.defense.gov/Portals/0/Documents/DIB%20CS-IA%20PIA_FINAL_signed_30jun2011_VMSS_GGMR_RC.pdf
[4] *See* Interim rule at http://www.gpo.gov/fdsys/pkg/FR-2012-05-11/pdf/2012-10651.pdf. To participate in the DIB CS/IA Program, the DIB company must own or operate an unclassified information system that processes, stores, or transmits DoD information.
[5] *See* PIA at section 2g(2), "when the DoD is performing its analysis on files, it may discover PII (or other sensitive information) that had not been identified by the DIB company when the information was submitted. If this occurs, all investigative work involving that PII ceases, the DIB company is notified that the PII (or sensitive information) was discovered, and the DIB company provides guidance as to the disposition of that information."
[6] *See* DHS/NPPD/PIA-084, "Enhanced Cybersecurity Services (ECS)." The term commercial service provider (CSP) refers to a public or private company that transports information electronically in the wireline, wireless, Internet, cable, satellite, and managed services businesses. Any managed security service provider meeting the eligibility requirements may become a CSP.

implement the countermeasures on its own networks, or by meeting the requirements to become a DHS-approved CSP to offer the services to other DIB companies.

A. Privacy Assessment

The Fair Information Practice Principles (FIPPs)

The FIPPs are a widely accepted framework of privacy principles used in the evaluation and consideration of systems, processes, or programs that affect individual privacy. The FIPPs provide the general basis for The Privacy Act of 1974, as amended, and many other privacy related laws and policies. The FIPPs are:

- **Transparency**: Organizations should be transparent and notify individuals regarding collection, use, dissemination, and maintenance of PII.
- **Individual Participation**: Organizations should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII. Organizations should also provide mechanisms for appropriate access, correction, and redress regarding use of PII.
- **Purpose Specification**: Organizations should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.
- **Data Minimization**: Organizations should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).
- **Use Limitation**: Organizations should use PII solely for the purpose(s) specified in the notice. Sharing PII should be for a purpose compatible with the purpose for which the PII was collected.
- **Data Quality and Integrity**: Organizations should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete.
- **Security**: Organizations should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.
- **Accountability and Auditing**: Organizations should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

The following table evaluates each FIPP with questions and answers regarding DIB CS/IA Program compliance:

Evaluation of DIB CS/IA Program by FIPP

1. Transparency	Response
How is the general public informed about the DIB CS/IA Program and information collection?	The public is informed about the DIB CS/IA Program and information collection in the following: • The DIB CS/IA Program SORN is DCIO 01. The SORN informs the public about the collection, maintenance, and use of information about an individual, where the records can be retrieved by the name of the individual or by some other type of identifier unique to the individual.[7] • The DIB CS/IA Program PIA.[8] The PIA assesses the impact on privacy for systems that collect PII. • The DIB CS/IA Program is governed by 32 C.F.R. Part 236, "[DoD-DIB] Voluntary Cyber Security and Information Assurance (CS/IA) Activities," which is subject to Federal rulemaking procedures, including publication for public comment.[9] In addition, there is a PAS provided to each DIB company POC at the point of collection for the POC PII.
For collections involving PII[10], how do affected individuals receive notice regarding the maintenance[11] of their PII?	For the POC PII, affected individuals receive notice in the following ways: • The DIB CS/IA Program SORN DCIO 01[12] identifies whose information is collected, the types of information collected, the purpose for the collection, routine uses of the information, how it is retrieved, and what safeguards are in place. • The DIB PIA states[13], "When the DIB company POC information is intentionally collected directly from an individual who is being designated as a POC, he/she is provided with the opportunity to consent or not consent to specific uses of PII when they are presented with the Privacy Act Statement."

[7] *See* SORN.
[8] *See* PIA.
[9] *See* Interim rule.
[10] For purposes of this assessment, the term PII is defined in OMB Memorandum M-07-16.
[11] See 5 U.S.C. 552a(a)(3). For purposes of this assessment, maintenance includes the collection, use, maintenance, dissemination, and disposition of PII.
[12] *See* SORN.
[13] *See* PIA at section 2j(1).

Evaluation of DIB CS/IA Program by FIPP

How does the DIB CS/IA Program ensure that notices are updated to reflect system or program changes?	The DIB CS/IA Program SORN was published in May 2012. DoD SORNs are reviewed every two years. The interim final rule for the DIB CS/IA Program[14] was published in May 2012. The final rule[15] for the program was published in October 2013.
Is the PIA summary available to members of the public on the DIB or DoD website?	Yes, the DIB CS/IA Program PIA summary is available to the public on the DoD website.[16]
Does the DIB CS/IA Program maintain an accounting of disclosures made to non-DoD individuals from the applicable system of records[17]?	No, PII is not disclosed as a part of the DIB CS/IA Program.
Please describe any barriers to ensure continued transparency of the program and its maintenance of PII.	32 C.F.R. Part 236, "Department of Defense (DoD)-Defense Industrial Base (DIB) Voluntary Cyber Security and Information Assurance (CS/IA) Activities,"[18] provides general information about the program. It points out that "Pursuant to established procedures and applicable regulations, the Government will protect sensitive nonpublic information under this program against unauthorized public disclosure by asserting applicable FOIA exemptions and will inform the non-Government source or submitter (e.g., DIB participants) of any such information that may be subject to release in response to a FOIA request, to permit the source or submitter to support the withholding of such information or pursue any other available legal remedies."

[14] *See* Interim Final Rule at http://www.gpo.gov/fdsys/pkg/FR-2012-05-11/pdf/2012-10651.pdf.
[15] *See* Final Rule at http://www.regulations.gov/#!documentDetail;D=DOD-2009-OS-0183-0014.
[16] *See* PIA.
[17] *See* 5 U.S.C. 552a (a)(5). A system of records is a group of records under the control of a DoD Component from which PII about an individual is retrieved by the name of the individual, or by some other identifying number, symbol, or other identifying particular assigned, unique to the individual.
[18] *See* 32 C.F.R. part 236, http://www.fas.org/sgp/news/2012/05/cyber-dib.html.

When collecting information from members of the public, does the program submit documentation for an OMB Collection number? If so, please provide the OMB Collection Number.	Yes, there are two OMB Control Numbers for the DIB CS/IA Program, 0704–0490 (POC PII) and 0704–0489 (CS/IA Cyber Incident Reporting). They were both submitted for reinstatement on August 30, 2013.[19]

[19] *See* http://www.gpo.gov/fdsys/pkg/FR-2013-08-30/pdf/2013-21234.pdf.

2. Individual Participation	Response
Are individuals asked for consent and given the opportunity to object to the collection of their PII?	Yes, the DIB CS/IA PIA states, "When the DIB company POC information is intentionally collected directly from an individual who is being designated as a POC, he/she can object to the collection of PII at that time."
Are individuals given the opportunity to access and correct their PII?	Yes, DIB company POCs can find instructions about how to access and correct their PII in the DIB CS/IA SORN.
Describe the mechanism provided for an individual to seek redress in the event of inappropriate access to or disclosure of their PII.	The DIB CS/IA SORN states, "The OSD rules for accessing records, for contesting contents, and appealing initial agency determinations are published in OSD Administrative Instruction 81; 32 CFR Part 311; or may be obtained from the system manager."
What steps are taken to ensure information maintained in the system is accurate, timely, relevant, and complete?	DIB CS/IA Program staff periodically review the data and it is incumbent upon the DIB company to provide accurate and updated POC information.
Is the provision of PII mandatory or voluntary? If mandatory, please cite the specific policy or guidance that requires the collection as well as rules and outcomes for failing to provide information.	For the POC PII, the disclosure is voluntary. The program's PAS states, "However, failure to provide requested information may limit the ability of the DoD to contact the individual or provide other information necessary to facilitate this program."
Is PII collected directly from the individual or from a third party? If from a third party, please describe how the program ensures the information is accurate and complete.	For POC PII, the DIB companies provide the information about their POCs. As part of the administrative management of the DIB CS/IA Program, each participating DIB company provides basic identifying information for a limited number of its personnel who are authorized to serve as the primary company POCs. The information provided for each POC includes business contact information (e.g., name, title, organizational unit, business email and phone), plus additional information necessary to verify the individual's authorization to receive classified information or controlled unclassified information (e.g., security clearance, citizenship). This information is required by the DIB CS/IA Program office to manage the program and interact with the companies through routine emails, phone calls, and participation in periodic classified meetings. A DIB company that is not yet participating in the program may also provide POC information to the DIB CS/IA Program office in order to discuss the program, including application procedures or to

	receive information about the program. Inadvertently collected PII is not collected from the individual. It is provided by a DIB company regarding a specific cyber incident. This PII is incidental to, or embedded in, the information being shared for cyber security analysis.

3. Purpose Specification	Response
Please provide the specific purpose(s) for the maintenance of PII within the system.	The DIB CS/IA Program SORN states: "To facilitate the sharing of DIB CS/IA cyber threat information and best practices to DIB companies to enhance and supplement DIB participant capabilities to safeguard DoD information that resides on, or transits, DIB unclassified information systems. When incident reports are received, DoD Cyber Crime Center (DC3) personnel analyze the information reported for cyber threats and vulnerabilities in order to develop response measures as well as improve government and DIB understanding of advanced cyber threat activity. DoD may work with a DIB company on a more detailed, digital forensics analysis or damage assessment, which may include sharing of additional electronic media/files or information regarding the incident or the affected systems, networks, or information." Further DIB CS/IA Program PAS states, "Purpose: Administrative management of the DIB CS/IA Program's information sharing activities. Personal information is discussed in SORN DCIO 01.[20]
What steps are taken to ensure the authority for the collection is valid?	Authority is provided for by 32 CFR Part 236.[21]

[20] *See* SORN.
[21] *See* 32 C.F.R. part 236.

4. Data Minimization	Response
Please describe the data elements that are relevant and necessary.	The DIB CS/IA PIA lists the following POC PII: name, citizenship, security clearance, business email, and business telephone number. Although it is not typical or expected, there exists the potential that information provided by a DIB company regarding a specific cyber incident may include PII that is incidental to, or embedded in, the information being shared for the cyber security analysis. This information is shared with DoD only if the DIB company determines that the PII is relevant to the incident response and analysis. Any such inadvertently collected PII submitted by DIB companies is reviewed by DC3 personnel to determine whether that PII is necessary for subsequent analysis in furtherance of its DIB CS/IA activities before such data is further processed or retained. PII deemed unnecessary for subsequent analysis is purged from DC3 systems.
Please describe how the program removes data that is no longer necessary for the system.	The DIB company POC information provided to support the DIB CS/IA Program administration and management process is maintained only as long as the designated POC(s) continues to represent the participating company. When the DIB CS/IA Program office is notified that a DIB company POC was replaced, the POC information is updated and outdated PII is archived in accordance with records management requirements. Inadvertent PII deemed unnecessary for subsequent analysis is purged. Inadvertently collected PII determined to be relevant is maintained, controlled, and disposed of when no longer reasonably necessary for intrusion investigation, forensics analysis, and damage assessment activities (or other legal, audit, or operational purposes).
Are records maintained in accordance with National Archives and Records Administration retention and disposal schedules? If so, please describe any applicable schedules.	The DIB CS/IA PIA states, "In accordance with NARA regulation and 32 C.F.R. Parts 1220-1239, program records are retained for a minimum of three (3) years, and tracking/ticketing system records are retained for a minimum of two (2) years." The final disposition of the retention and disposal schedule is pending with NARA. Inadvertent PII is not covered by a NARA retention and disposal schedule. Inadvertent PII deemed unnecessary for subsequent analysis is purged. Inadvertently collected PII determined to be relevant is maintained, controlled, and disposed of when no longer reasonably necessary for intrusion investigation, forensics analysis, and damage assessment activities (or other legal, audit, or operational purposes).

Evaluation of DIB CS/IA Program by FIPP

Please describe the method for ensuring that only the minimum necessary amount of data is collected.	The information sharing activities covered by the DIB CS/IA PIA are focused on sharing cyber security related information, and the program seeks to minimize the collection and management of PII except as necessary to support the program. The operational implementation of this sharing arrangement involves sharing and managing PII in two ways: For program administration and management purposes, the DIB companies share with DoD typical business contact information for its personnel who are serving as company POCs for the program. For cyber incident response and analysis purposes, although it is not typical or expected, there exists the potential that information provided by a DIB company regarding any specific cyber incident may include PII that is incidental to, or embedded in, the information being shared for cyber security analysis. This information is shared with DoD only if the DIB company determines that the PII is relevant to the incident response and analysis.

Evaluation of DIB CS/IA Program by FIPP

5. Use Limitation	Response
Please describe the steps taken to ensure the use of PII is limited to the purpose(s) specified in applicable notices.	The DIB CS/IA Program collects DIB company POC PII only for routine program administration and management purposes. This PII does not involve any particularly sensitive personal information – it is limited to the individual's contact information that is routinely shared in the ordinary course of business (e.g., name, title, organizational division, business email and phone), and includes other information (e.g., security clearance, citizenship) that is necessary to verify the individual's authorization to receive classified or other controlled unclassified information under the program. Inadvertently collected PII that may be submitted by DIB companies in connection incident reporting and response is reviewed by DC3 personnel to determine whether that PII is necessary for subsequent analysis. Information deemed unnecessary for subsequent analysis is purged from DC3 systems.
Please describe any steps taken to mitigate any use of PII that is not specified in the applicable notices.	Inadvertently collected PII is provided to DoD by a participating DIB company based on that company's determination that the PII is relevant to incident response and analysis, and that there are no legal, contractual, or other restrictions on sharing that PII with the government. Inadvertently collected PII submitted by DIB companies in connection with incident reporting and response is reviewed by DC3 personnel to determine whether that PII is necessary for subsequent analysis in furtherance of its DIB CS/IA Program activities. Information deemed unnecessary for subsequent analysis is purged from DC3 systems. Information determined to be relevant is maintained, controlled, and disposed of when no longer reasonably necessary for intrusion investigation, forensics analysis, and damage assessment activities (or other legal, audit, or operational purposes). The length of cyber-intrusion forensics analysis and damage assessments varies.

Evaluation of DIB CS/IA Program by FIPP

6. Data Quality and Integrity	Response
What steps are taken to ensure the continued quality and integrity of data maintained within system?	While the DIB CS/IA Program staff periodically review POC PII, and it is incumbent upon the DIB company to provide accurate and updated POC information.
Please describe steps that are taken to ensure the continued confidentiality, availability, and integrity of PII maintained within the system.	Although the name of a DIB company, its program, or the POC PII, might not by itself be sensitive, the association of that company or its specific POCs with particular cyber security activities, or with particular cyber security incidents, may be treated as sensitive. Accordingly, the DIB CS/IA Program restricts access to such PII only to those authorized personnel who have a need to know for duties in support of the program, and are subject to strict nondisclosure obligations. PII inadvertently collected is maintained with strict need to know and access control by DoD to government and government contractor personnel who have signed a non-disclosure agreement. An unclassified standalone network supports the analysis of malware in files provided by DIB partners, while a classified standalone network hosts the information provided by DIB partners for cyber intrusion damage assessment. Data is purged when no longer needed.
Please describe the method for eliminating PII that is no longer needed.	DIB company POC PII provided to support the DIB CS/IA Program administration and management is maintained only as long as the designated POC continues to represent the participating DIB company. When the DIB CS/IA Program office is notified that a POC was replaced, the POC information is updated and outdated PII is archived in accordance with records management requirements. Inadvertent PII deemed unnecessary for subsequent analysis is purged. Inadvertently collected PII determined to be relevant is maintained, controlled, and disposed of when no longer reasonably necessary for intrusion investigation, forensics analysis, and damage assessment activities (or other legal, audit, or operational purposes).

7. Security	Response
Please describe any safeguards that are in place to ensure the continued security of data maintained within the system.	The published SORN DCIO 01 states, "Records are accessed by DIB CS/IA Program office and DC3 personnel with security clearances who are properly screened, trained, under a signed confidentiality agreement, and determined to have 'need to know'. Access to records requires DoD Common Access Card (CAC) and PIN. Physical access controls include security guards, identification badges, key cards, cipher locks, and combination locks." In addition, the published PIA available to the public states, "There are minimal risks associated with the PII collected in connection with the DoD-DIB cyber security information sharing activities under the DIB CS/IA Program. The Program's information sharing activities implements administrative, technical, and electronic protections to ensure compliance with all applicable DoD policies and procedures regarding the collection and handling of PII and other sensitive information."
Please describe the method for securing data at rest in the system.	The published PIA available to the public states, "All DoD information systems used to process and store PII (or any sensitive information) have undergone a mandatory certification and accreditation process to verify that the system provides adequate measures to preserve the authenticity, integrity, availability, and confidentiality of all sensitive information residing or transiting those systems.[22] In addition, DC3 undergoes extensive inspection by the American Society of Crime Lab Directors to ensure that DC3 information handling procedures are reliable, valid, and repeatable in accordance with standards necessary for accreditation as a digital forensics laboratory."
Please describe the method for ensuring data in transit is appropriately secured.	The published PIA available to the public states, "All DoD information systems used to process and store PII (or any sensitive information) have undergone a mandatory certification and accreditation process to verify that the system provides adequate measures to preserve the authenticity, integrity, availability, and confidentiality of all sensitive information residing or transiting those systems.[23] In addition, DC3 undergoes extensive inspection by the American Society of Crime Lab Directors to ensure that DC3 information handling procedures are reliable, valid, and repeatable in accordance with standards necessary for accreditation as a digital forensics laboratory."

[22] *See* http://www.dtic.mil/cjcs_directives/cdata/unlimit/8010_01.pdf.
[23] *Id.*

Please describe the method for ensuring that access to data maintained within the system is limited to individuals with a need to know.	The published SORN DCIO 01 states, "Records are accessed by DIB CS/IA Program office and DC3 personnel with security clearances who are properly screened, trained, under a signed confidentiality agreement, and determined to have need to know."
If data from the system is sent electronically, what methods are in place to ensure appropriate safeguards apply?	All data that is sent from the system is encrypted per DoD standards. Access to the system is very limited, and all users are required to sign a Non-Disclosure Agreement before being granted access to the system.
Has PII within the system of records been categorized to reflect low, moderate, or high impact PII?	Yes, PII within the system was categorized as low impact. The Department established policy for categorizing PII in DoD CIO Memo, "DoD Guidance on Protecting PII," August 18, 2006.[24]
What methods are in place to mitigate and address identified vulnerabilities to records maintained within the system?	The system is certified and accredited in accordance with DoD policy. DoD is required by statute to establish programs and activities to protect DoD information and DoD information systems, including information and information systems operated and maintained by contractors or others in support of DoD activities. Section 2224 of title 10, U.S. Code (U.S.C.),[25] requires DoD to establish a Defense IA Program to protect and defend DoD information, information systems, and information networks that are critical to the Department during day-to-day operations and operations in times of crisis.[26] The program must provide continuously for the availability, integrity, authentication, confidentiality, non-repudiation, and rapid restitution of information and information systems that are essential elements of the Defense information infrastructure.[27] The program strategy also must include vulnerability and threat assessments for defense and supporting non-defense information infrastructures, joint activities with elements of the national information infrastructure, and coordination with representatives of those national critical infrastructure systems that are essential to DoD operations.[28] The program must

[24] *See* http://dpclo.defense.gov/privacy/documents/DODGuidancePII.pdf
[25] *See* http://www.gpo.gov/fdsys/pkg/USCODE-2010-title10/pdf/USCODE-2010-title10-subtitleA-partIV-chap131-sec2224.pdf.
[26] *Id.* at (a).
[27] *Id*. at (b).
[28] *Id.* at (c).

	provide for coordination, as appropriate, with the heads of any relevant federal agency and with representatives of those national critical information infrastructure systems that are essential to the operations of the Department regarding information assurance measures necessary to the protection of these systems.[29] The Defense IA Program also must ensure compliance with federal IA requirements provided in the Federal Information Security Management Act (FISMA).[30] FISMA requires all federal agencies to provide information security protections for information collected or maintained by or on behalf of the agency; and information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.[31] Agencies are expressly required to develop, document, and implement programs to provide information security for information and information systems that support the operations and assets of the agency, including those provided by another agency, contractor, or other source.[32]
Briefly describe the methodology for responding to and mitigating issues related to any potential breach of PII.	The DIB CS/IA Program office follows DoD's breach reporting and mitigation policies and procedures in section C.1.5 of DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007.[33]
How are individuals with a need to know provided access to data maintained within the system of records?	Collection of PII in support of DIB CS/IA Program administrative management is provided by the DIB participating companies through DoD approved Public Key Infrastructure certificates. Inadvertently collected PII is maintained on an unclassified standalone network supporting the analysis of malware in files provided by DIB partners, while a classified standalone network hosts the media provided by DIB partners for cyber intrusion damage assessment. Access is strictly controlled by DoD to personnel with a need to know and who have signed a non-disclosure agreement.

[29] *See* http://www.gpo.gov/fdsys/pkg/USCODE-2010-title10/pdf/USCODE-2010-title10-subtitleA-partIV-chap131-sec2224.pdf.
[30] *See* 44 U.S.C. §§ 3541 *et seq*., http://www.gpo.gov/fdsys/pkg/USCODE-2008-title44/pdf/USCODE-2008-title44-chap35-subchapIII-sec3541.pdf.
[31] *Id*. at (a)(1)(A).
[32] *Id.* at (b).
[33] *See* DoD 5400.11-R, http://www.dtic.mil/whs/directives/corres/pdf/540011r.pdf.

8. Auditing and Accountability	Response
What methods are in place to audit access to records maintained within the system?	The system is hosted and monitored by the Defense Information Systems Agency. As part of program oversight, audit trails and user access can be reviewed.
Please describe any agency oversight mechanisms that apply to the system.	The DIB CS/IA Program and its optional DECS component were reviewed by the Defense Privacy and Civil Liberties Office and the DoD Office of General Counsel. The collection, retention, and dissemination of PII by DoD intelligence or counterintelligence components is in accordance with the Attorney General Guidelines of 1982 contained in DoD 5240.1-R.[34] All DoD information systems used to process and store PII (or any sensitive information) have undergo a mandatory certification and accreditation process to verify that the system provides adequate measures to preserve the authenticity, integrity, availability, and confidentiality of all sensitive information residing or transiting those systems.[35] In addition, DC3 undergoes extensive inspection by the American Society of Crime Lab Directors to ensure that DC3 information handling procedures are reliable, valid, and repeatable in accordance with standards necessary for accreditation as a digital forensics laboratory. None of these DIB CS/IA Program activities involve any DoD or government personnel performing any monitoring of a DIB company or other private networks. DIB companies are responsible for monitoring their own networks and for ensuring that there are no legal, contractual, or other restrictions on sharing PII or any other sensitive information with DoD. The only PII received by DoD under these activities is PII that is provided directly to DoD by authorized DIB company personnel. PII inadvertently collected is maintained with strict need to know and access control by DoD to government and government contract personnel who have signed a nondisclosure agreement. An unclassified stand-alone network supports the analysis of malware in files provided by DIB companies, while a classified standalone network

[34] *See* http://www.dtic.mil/whs/directives/corres/pdf/524001r.pdf.
[35] *See* http://www.dtic.mil/cjcs_directives/cdata/unlimit/8010_01.pdf.

	hosts information provided by DIB companies for cyber intrusion damage assessment. Data is purged when no longer needed.
Please describe methods that are in place to audit compliance with applicable laws and policies that pertain to the system.	32 CFR Part 236[36] provides authority for the program and POC PII collections. Any change to this rule requires active participation of the DIB CS/IA Program.
Please describe the methodology to ensure that only PII relevant to the system is maintained within the system.	The DIB CS/IA Program is structured around several key elements that are designed to ensure that risks are effectively addressed to safeguard privacy: • All POC PII received by the DoD is provided voluntarily by authorized DIB company representatives, subject to mutually agreed upon restrictions; • The nature of the PII being intentionally collected is limited to ordinary business contact information for DIB company personnel; • Other PII inadvertently collected is submitted only if a DIB company has determined that the PII is relevant to cyber incident response and analysis activities, and that the PII is authorized to be shared with the DoD for these purposes; • Once collected, access and use of PII is limited to authorized personnel that need to know and is otherwise lawful; • All DIB CS/IA Program and supporting personnel receiving access to the collected PII are required to undergo training and are subject to appropriate non-disclosure restrictions; and • PII is maintained for only as long as necessary for DIB CS/IA Program activities and is managed and disposed of in accordance with applicable records management requirements.
Please describe any methods to ensure continued compliance with the FIPPs.	Continued DIB CS/IA Program compliance with DoD Directive 5400.11,[37] "DoD Privacy Program," May 8, 2007 and DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007 will ensure FIPP compliance.

[36] *See* http://www.fas.org/sgp/news/2012/05/cyber-dib.html.
[37] *See* http://www.dtic.mil/whs/directives/corres/pdf/540011p.pdf.

B. Civil Liberties Assessment

In this section, civil liberties protections in the DIB CS/IA Program are assessed under the DoD Civil Liberties Program, DoD policies, and the First and Fourth Amendments to the Constitution of the United States.

DoD Civil Liberties Program[38]

Civil liberties are defined as fundamental rights and freedoms protected by the Constitution of the United States. These freedoms protect individuals from improper government activity and are guaranteed by the Bill of Rights, the first ten Amendments to the U.S. Constitution. Examples include freedom of speech, press, or religion; due process of law; and other limitations on the power of the government to restrain or dictate the actions of individuals.

To ensure DoD adequately considers civil liberties in its activities, the DoD Civil Liberties Officer created the Defense Privacy and Civil Liberties Office and the DoD Civil Liberties Program. Under DoD Instruction 1000.29, "DoD Civil Liberties Program," the DoD Civil Liberties Principles are:

1. Civil liberties are fundamental rights and freedoms protected by the Constitution of the United States.
2. The Department of Defense will protect the civil liberties of DoD employees, members of the Military Services, and the public to the greatest extent possible, consistent with its operational requirements.
3. The Department of Defense will consider appropriately civil liberties in the review, development, and implementation of new or existing laws, regulations, policies, and initiatives.
4. No information shall be maintained on how an individual exercises rights protected by the First Amendment to the Constitution of the United States, including the freedoms of speech, assembly, press and religion, except when:

    - Specifically authorized by statute;
    - Expressly authorized by the individual, group of individuals, or association on whom the record is maintained; or
    - The record is pertinent to and within the scope of an authorized law enforcement, intelligence collection, or counterintelligence activity.

[38] DoD Instruction 1000.29, "DoD Civil Liberties Program," May 17, 2012. http://www.dtic.mil/whs/directives/corres/pdf/100029p.pdf.

The DIB CS/IA Program must adhere to the principles and the DoD Civil Liberties Program, generally.

The DoD Civil Liberties Program also ensures that adequate procedures exist to receive, investigate, respond to, redress, and report complaints which allege that a violation of civil liberties was committed by any DoD program, including the DIB CS/IA Program. DoD has not received any civil liberties complaints concerning the activities of the DIB CS/IA Program.

Constitutional Issues

The DIB CS/IA Program safeguards civil liberties guaranteed by the First and Fourth Amendments to the U.S. Constitution.

Fourth Amendment

The Fourth Amendment to the U.S. Constitution ensures protection from unreasonable government searches and seizures.[39] A search is any intrusion by the government into something in which one has a reasonable expectation of privacy.[40] Courts generally recognize a legitimate expectation of privacy in the content of private online conversations while in transmission; therefore, government monitoring of the content of these communications could imply a government search.[41] A government search that is conducted without judicial authorization is "per se unreasonable" under the Fourth Amendment, subject only to specifically established exceptions.[42]

The DIB CS/IA Program enables participating DIB companies to effectively share cyber threat information with DoD to address cyber threats to unclassified DoD information transiting or residing on DIB information systems and networks.[43] The DIB CS/IA Program increases DoD and DIB company awareness regarding the extent and severity of advanced persistent threats, and establishes a comprehensive approach for protecting DoD information from such threats.[44]

The DIB CS/IA Program does not violate the Fourth Amendment because DoD does not monitor private online conversations or share PII to facilitate a government search against an individual; it only shares information to address cyber threats.

---

[39] U.S. CONST. amend. IV.
[40] *See Katz v. United States*, 389 U.S. 347 (1967).
[41] *See, e.g., United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010) (holding there is a reasonable expectation of privacy in the contents of emails sent or received through, or stored with, a Commercial Service Provider).
[42] *Katz*, 389 U.S at 357.
[43] DoD Instruction 5205.13 "Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/IA) Activities," January 29, 2010.
[44] DoDI 5205.13 defines "advanced persistent threats" as threats from extremely proficient, patient, determined, and capable adversary(ies).

There are only two specific circumstances under which DIB companies voluntarily provide any information to DoD, neither of which involves government monitoring of private online conversations or enables a government search against an individual.

The first circumstance arises when the DIB company voluntarily provides PII to DoD for program administration and management purposes.[45] DIB companies share with DoD business contact information for its personnel that are serving as the company points of contact for the program.[46] Providing routine business contact information does not implicate the Fourth Amendment.

The second instance occurs when DIB companies voluntarily provide DoD with information for cyber incident response and analysis purposes.[47] The information shared with DoD by the DIB company does not involve government monitoring of private online conversations and is not collected as part of a government search. Instead, it is voluntarily provided to DoD by the DIB company, based on the company's own interdependent cyber security activities and the company's determination that the information is relevant to the incident response and analysis, and that the information has been obtained, and is being shared, lawfully.[48] The sharing of this cyber threat information enables the program to achieve its goal of increasing DoD and DIB company awareness of cyber threats to DoD information on DIB company networks.

Although it is not typical or expected, it is possible that some of the information about a specific cyber incident may include PII that is incidental to, or embedded in, the information the DIB company has shared with DoD for cyber security analysis. DIB companies share this PII with DoD only after the company determines there are no legal, contractual, or other restrictions on sharing it with DoD for cyber incident response and/or analysis purposes.[49] When PII is shared, safeguards exist to protect against unauthorized use of the PII. This includes privacy safeguards that limit dissemination to those with a need-to-know the information.[50] DoD's receipt of this inadvertent PII does not constitute a search under the Fourth Amendment and the activities of the DIB CS/IA Program do not otherwise violate the Fourth Amendment.

---

[45] *See* PIA.
[46] *Id*.
[47] *Id*.
[48] *See* 32 CFR 236.6(c), "Prior to sharing any information with the Government under this program … the DIB participant shall perform a legal review of its policies and practices that support its activities under this program, and shall make a determination that such policies, practices, and activities comply with applicable legal requirements."
[49] *See* PIA.
[50] *Id*.

First Amendment

The First Amendment prohibits Congress from passing any law that prohibits the free exercise of religion or abridges freedom of speech, freedom of the press, the right of people to assemble peaceably, or the right to petition the government for redress of grievances.[51]

The DIB CS/IA Program does not violate a person's First Amendment rights because it does not collect or share information on how an individual exercises rights protected by the First Amendment.

The DIB CS/IA Program increases DoD and DIB company awareness regarding the extent and severity of advanced persistent threats, and establishes a comprehensive approach for protecting DoD information from such threats.[52]

As discussed, DIB companies volunteer information to DoD in two limited instances. Neither of these instances involves the collection or sharing of information by DoD that "chills" free speech or free association.

First, DIB companies provide PII for program administration and management purposes. This PII is limited to routine business contact information of DIB company personnel (*e.g.*, name, title, organizational division, business email, phone number) and security clearance and citizenship information, and does not include any speech or information about the exercise of any right.

Second, DIB companies voluntarily share information with DoD for cyber incident response and analysis purposes.[53] The DIB CS/IA Program does not ask for any information about how individuals exercise their First Amendment rights. In the extremely unlikely event that information shared for cyber incident response and analysis purposes contains information about how an individual exercises their First Amendment rights, the DIB CS/IA Program will apply appropriate handling safeguards.[54] This includes the use of uniform procedures and safeguards to ensure that inadvertently collected information is maintained in compliance with strict need-to-know access controls.[55] DoD does not use data provided by the DIB companies for any other purpose except in furtherance of the DIB CS/IA Program mission and under no circumstance is program data used to impinge on First Amendment protected rights.

---

[51] U.S. CONST. amend. I.
[52] DoDI 5205.13.
[53] *See* PIA.
[54] *Id.*
[55] *Id.*

Conclusion

The DIB CS/IA Program is a cooperative cyber security program for the benefit of DoD and those companies that volunteer to participate in it. The operation of the program neither violates the First nor Fourth Amendment and the program complies with existing DoD Civil Liberties Program policy. Based on the purpose, design, and function of the program, appropriate civil liberties protections are incorporated into the DIB CS/IA Program.

PART IV

DEPARTMENT OF JUSTICE

U.S. Department of Justice

Office of the Deputy Attorney General

Telephone: (202) 514-2101 *Washington, D.C. 20530*

December 6, 2013

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security

Megan H. Mack
Officer for Civil Rights and Civil Liberties
Department of Homeland Security

Dear Ms. Neuman and Ms. Mack:

On behalf of the Department of Justice and in accordance with Section 5(b) of Executive Order 13636, I am pleased to submit the enclosed privacy and civil liberties assessment of the Department's activities under the Executive Order. As the Department's Chief Privacy and Civil Liberties Officer, I am providing this assessment to the Department of Homeland Security for consideration and inclusion in its publicly available privacy and civil liberties report.

We appreciate the efforts of your respective staffs to lead this consolidated response for the federal government. If you have any questions about the Department of Justice's contribution to the report, please do not hesitate to contact me.

Sincerely,

Erika Brown Lee
Chief Privacy and Civil Liberties Officer

Enclosure

United States Department of Justice

THE CHIEF PRIVACY AND CIVIL LIBERTIES OFFICER AND THE OFFICE OF PRIVACY AND CIVIL LIBERTIES

INITIAL PRIVACY AND CIVIL LIBERTIES ASSESSMENT UNDER EXECUTIVE ORDER 13636

February 12, 2013 – December 6, 2013

I. Introduction

Section 5 of Executive Order 13636 requires agencies to coordinate their activities with their department Senior Agency Officials for Privacy and Civil Liberties (SAOPCLs) to: 1) incorporate privacy and civil liberties protections into departmental activities implementing the Executive Order that improve cybersecurity for U.S. critical infrastructure; and 2) conduct assessments of those activities, based on the Fair Information Practice Principles (FIPPs) and other applicable policies, principles and frameworks.[1] SAOPCLs are also required to provide written assessments of implementing activities to the Department of Homeland Security (DHS) pursuant to Section 5(b) of the Executive Order. Accordingly, the Department of Justice ("DOJ" or "the Department") submits this privacy and civil liberties assessment of the Department's implementing activities to DHS for its consideration and inclusion in its public report. The reporting period for this assessment covers the timeframe from February 12, 2013, to December 6, 2013.

II. Implementation of Section 4(a)

Section 4(a) of the Executive Order requires the Attorney General, within 120 days of the date of the Executive Order, to issue instructions to ensure the timely production of unclassified reports of cyber threats to the U.S. homeland that identify a specific targeted entity, consistent with his authority and with the requirements of Section 12(c) of the Executive Order. The instructions are to address the need to protect intelligence and law enforcement sources, methods, operations, and investigations.

On June 12, 2013, the Deputy Attorney General signed a Department Order issuing instructions regarding the timely production of unclassified reports of cyber threat information to Department components pursuant to Section 4(a) of the Executive Order. Specifically, the Order requires the timely production of unclassified reports of cyber threats to the U.S. homeland that identify a specific targeted entity, and also instructs that all actions taken pursuant to the Order be consistent with the need to protect privacy and civil liberties.[2]

III. Implementation of Section 4(b)

Section 4(b) of the Executive Order requires the Attorney General and the Secretary of DHS, in coordination with the Director of National Intelligence, to establish a process that rapidly disseminates cyber threat reports to targeted entities. Additionally, Section 5 of the Executive Order establishes a privacy and civil liberties protection and oversight cycle. All of the steps of the cycle are based upon, and evaluating activities against, the Fair Information Practice Principles and other applicable policies, principles and frameworks to protect individual privacy and civil liberties.[3]

---

[1] Executive Order No. 13636, *Improving Critical Infrastructure Cybersecurity* (Feb. 12, 2013), *available at* http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.

[2] For further information, see the Department Order, which is attached hereto.

[3] Fair Information Practice Principles (FIPPs) are the widely-accepted framework of defining principles used to assess and mitigate privacy and civil liberties impacts of information systems, processes, or programs.

In late 2012, the FBI began developing iGuardian, an unclassified web portal designed to accept cyber intrusion complaints from the private sector. Similar to the incident tickets created for the U.S. government's incident and breach reporting, iGuardian uses a web form portal to collect information about a potential cybersecurity incident from known, trusted partners. As currently envisioned, iGuardian would be one part of the plan currently under development to implement Section 4(b). While the implementation plan is still evolving, it is also envisioned that other federal agencies would have access to and share cyber information through the Guardian database. [4]

Although the portal is not currently fully developed, the FBI plans to develop a centralized reporting and notification tool that will allow trusted partners to report cyber incidents in real time. At present, iGuardian serves as a complaint portal to transmit cyber reports to the FBI for possible review. Currently, all users of iGuardian are trusted members who voluntarily provide information through InfraGard, a public-private partnership between the FBI and members of the private sector who are focused on intrusions and vulnerabilities affecting the critical infrastructure sectors.

Any entity wishing to submit suspicious cyber reports to iGuardian must first submit an application to the FBI to become a trusted InfraGard partner. Once the FBI has vetted the application and determined the entity is a trusted partner, the user can log in to iGuardian through InfraGard. The vetting of applicants ensures that only known and trusted partners can submit information through the portal. Upon initial login, all portal users are shown a notice banner indicating the purpose of iGuardian in order to provide notice and transparency about the information collected by the portal. The information that may be collected through the portal includes names of individuals associated with the complaint, internet protocol addresses, and/or other information provided by the complainant in the comments form or uploaded as an attachment.

Upon receipt of the complaint, iGuardian itself does not store any of the information provided in the complaint; the information is forwarded to another FBI system, Guardian,[5] where each complaint is manually reviewed. The iGuardian incidents are reviewed by an FBI Cyber Watch investigator to determine if the incident warrants additional action. If the incident warrants additional action because it is deemed a credible complaint, it is assigned to the appropriate FBI entity for further review and investigation. All iGuardian information undergoes a manual review within Guardian to ensure that only relevant information is maintained. All other non-relevant information is purged from the Guardian system. As a result, all information transmitted by iGuardian is forwarded to Guardian for review, thereby ensuring that the data

[4] The FBI completed a privacy impact assessment (PIA) for Guardian in 2005. Because Guardian is a national security system, this PIA is not publicly posted. Guardian is covered by the system of records notice for the FBI Data Warehouse System, FBI-022, which is available at http://www.gpo.gov/fdsys/pkg/FR-2012-07-10/pdf/2012-16823.pdf.

[5] Guardian is an FBI system maintained at the Secret level that supports the FBI's role in defending the United States and its interests abroad from the threat of terrorism by receiving, assessing, disseminating and retaining information related to threats, suspicious activities and events with a potential nexus to terrorism.

collected is appropriately limited. Any information that is transferred to the FBI's Guardian system is covered by the privacy compliance documentation for Guardian.

The FBI is in the process of preparing a Privacy Threshold Analysis to determine if the iGuardian portal itself requires additional privacy compliance documentation. As iGuardian and Guardian undergo further developments, including for the purpose of fully implementing Section 4(b) of the Executive Order, the Department and the FBI will conduct a more comprehensive assessment of the privacy and civil liberties risks and include that assessment in future reports.

IV. Conclusion

As the Department engages in further activities under the Executive Order, the CPCLO will continue to coordinate with Department leadership and components to ensure that privacy and civil liberties protections are incorporated into such activities. The Department will review and revise this assessment as necessary to evaluate the privacy and civil liberties risks of cyber security activities.

Office of the Deputy Attorney General
Washington, D.C. 20530

ORDER NO. 3393-2013

ISSUING INSTRUCTIONS PURSUANT TO EXECUTIVE ORDER 13636 REGARDING THE TIMELY PRODUCTION OF UNCLASSIFIED REPORTS OF CYBER THREAT INFORMATION

By the authority vested in the Attorney General by 28 U.S.C. §§ 509, 510, and 533, and delegated to the Deputy Attorney General in 28 C.F.R. § 0.15(a), and in furtherance of the policy of the United States Government established in Executive Order 13636 of February 12, 2013, and pursuant to section 4(a) thereof, I hereby order that:

1. The Federal Bureau of Investigation (FBI), consistent with its authorities, including 18 U.S.C. § 1030, 28 C.F.R. § 0.85, Executive Order 12333 of December 4, 1981, as amended, Attorney General Guidelines for Domestic FBI Operations, National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (Jan. 9, 2008), and Presidential Policy Directive 21 (Feb. 12, 2013), shall produce on a timely basis unclassified reports of cyber threats to the U.S. homeland that identify a specific targeted entity (Cyber Threat Reports).

2. The FBI shall meet its obligation in section 1 of this order to produce timely Cyber Threat Reports through systems, reporting mechanisms, and guidance established to develop such reports, including FBI policy directives, implementing guidance related to the production of intelligence products, and, to the extent applicable, Intelligence Community Directive (ICD) 209 (Tearline Production and Dissemination), and any successor directive.

3. The FBI shall ensure that Cyber Threat Reports contain sufficient technical detail and threat context to facilitate the recipient's efforts to undertake network defense, incident response, remediation, and recovery and thereby promote the safety, security, and economic prosperity of the Nation and its cyber environment.

4. All other Components of the Department of Justice (Department) shall assess their systems, reporting mechanisms and guidance to ensure that, to the extent applicable, they are facilitating the timely production of Cyber Threat Reports, including through provision of the Component's relevant cybersecurity information to the FBI.

5. All Components of the Department shall, to the extent applicable, review and update their systems, reporting mechanisms, and guidance related to the timely production of Cyber Threat Reports as needed to ensure that the Department continues to promote the policy set forth in section 4(a) of Executive Order 13636 to increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities so that these entities may better protect and defend themselves against cyber threats.

6. All actions taken pursuant to this order shall be consistent with requirements and authorities to protect intelligence and law enforcement sources, methods, operations, and investigations, and with the need to protect privacy and civil liberties.

7. This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

6/12/13
Date

James M. Cole
Deputy Attorney General

PART V

DEPARTMENT OF COMMERCE

DATE: December 6, 2013

TO: Karen L. Neuman, Chief Privacy Officer, and
Megan H. Mack, Officer for Civil Rights and Civil Liberties
Department of Homeland

FROM: Catrina D. Purvis, Chief Privacy Officer
Department of Commerce's Office of Privacy
and Open Government

SUBJECT: Commerce Assessment of Executive Order (E.O.) 13636 – Improving Critical Infrastructure Cybersecurity

The Department of Commerce's (DOC) Chief Privacy Officer (CPO) has reviewed and completed a Privacy Assessment to examine the "Cybersecurity Framework" development activities performed by the National Institute of Standards and Technology (NIST). This assessment, conducted pursuant to Executive Order (E.O.) 13636 – Improving Critical Infrastructure Cybersecurity, directed federal departments and agencies to establish, expand, or prioritize activities to improve cybersecurity for the United State's critical infrastructure. Section 5 of the E.O. requires department and agency Senior Agency Officials for Privacy and Civil Liberties to incorporate privacy and civil liberties protection and conduct an assessment of those activities based on the Fair Information Practice Principles and any other applicable policies, principles, and frameworks.

Attached, in accordance with requested requirements, is the E.O. 13636 Cybersecurity Framework/Privacy and Civil Liberties Assessment report. If you have any questions, please contact Mr. Joey Hutcherson, via email at CPO@doc.gov.

Attachment: Commerce E.O. 13636 Privacy and Civil Liberties Assessment Report.pdf

United States Department of Commerce

E.O. 13636 - Privacy and Civil Liberties (CL) Assessment Report

The goal of the Commerce Privacy Program is to ensure Departmental policies and procedures regarding information protection are compliant with and adhere to all Privacy Laws, Mandates, and Best Practices.

Office of Privacy & Open Government

Privacy Program

December 2013

Department of Commerce
E.O. 13636 Privacy and Civil Liberties (CL)
Assessment Report

Executive Summary

The Department of Commerce (DOC) Chief Privacy Officer (CPO) completed a Privacy Assessment examining the "Cybersecurity Framework" development activities performed by the National Institute of Standards and Technology (NIST). This assessment was conducted pursuant to Executive Order (E.O.) 13636 – Improving Critical Infrastructure Cybersecurity which directs federal departments and agencies to establish, expand or prioritize a number of activities to improve cybersecurity for U.S. critical infrastructure. Section 5 of the E.O. requires department and agency Senior Agency Officials for Privacy and Civil Liberties[1] (SAOP/CLs) to incorporate privacy and civil liberties protection into such activities, and to conduct assessments of those activities based on Fair Information Practice Principles (FIPPs) and other applicable policies, principles and frameworks.

The primary DOC activity involving privacy risks was work performed under Section 7(a) of the E.O. which directs the NIST to lead the development of a Cybersecurity Framework. For this activity, the DOC CPO makes the following findings:

1. Cybersecurity Framework development efforts required NIST collection and processing of support contractor and conference/workshop registration related personally identifiable information (PII). Additionally, any PII submitted voluntarily during a public comment period was received and stored on NIST Information Technology (IT) systems. In all cases, the NIST ensured implementation of appropriate IT security and privacy protections. Accordingly, the level of privacy risk presented by these activities is Low[2] and in adherence with FIPPs.
2. No civil liberties risks/impacts were presented by Cybersecurity Framework development activities; thus none were assessed.

The DOC SAOP has accepted the CPO's findings, and will ensure full implementation of the following CPO recommendations:

1. Ensure appropriate privacy and civil liberties protections are incorporated and maintained in all future NIST Cybersecurity Framework development activities.
2. Conduct an assessment of privacy and civil liberties risks associated with the Privacy Methodology section of the Cybersecurity Framework upon NIST's public release of a final Cybersecurity Framework for comment in 2014.
3. Submit an assessment of any remaining E.O. directed DOC activities involving privacy and civil liberties risks to the Department of Homeland Security (DHS) for the 2014 Compiled E.O. SAOP/CL Public Report.

[1] The DOC does not have a designated Civil Liberties Officer.
[2] A Low risk is one in which the loss of confidentiality, integrity, or availability is expected to have a limited adverse effect on organizational operations, organization assets or individuals.

Department of Commerce
E.O. 13636 Privacy and Civil Liberties (CL)
Assessment Report

Table of Contents

Department of Commerce
E.O. 13636 Privacy and Civil Liberties (CL)
Assessment Report

1.0 Overview

The national and economic security of the United States depends on the reliable functioning of critical infrastructure. To strengthen the resilience of this infrastructure, President Obama issued Executive Order 13636 (E.O.) - Improving Critical Infrastructure Cybersecurity, dated February 12, 2013. The E.O. requires the development of a framework (the "Cybersecurity Framework") to reduce cybersecurity risks to critical infrastructure and to assist organizations responsible for critical infrastructure services with managing cybersecurity risk. The critical infrastructure community includes public and private owners, operators, and other entities that play a role in securing the Nation's infrastructure. Section 7(a) of the E.O. directs the National Institute of Standards and Technology (NIST) to lead the development of the Cybersecurity Framework in collaboration with industry. Accordingly, NIST issued Requests for Information (RFIs), received public comments, and held a series of public workshops. These activities involved the collection and processing of support contractor and conference/workshop registration related personally identifiable information (PII) that are subject to privacy protections afforded by the Privacy Act of 1974 and the Federal Information Security Management Act (FISMA). This document provides an analysis of privacy protections for the PII against the Fair Information Practice Principles (FIPPs).

2.0 E.O. Implementation Activity

The Cybersecurity Framework is being developed by NIST employees and contractors through a series of meetings with and requests for information from the public, followed by draft documents, and receipt of draft document comments from the public. The NIST published a Preliminary Cybersecurity Framework for public comment in October 2013. It relies on existing standards, guidance, and best practices to achieve outcomes that can assist organizations in managing their cybersecurity risk, and is a risk-based approach comprised of the following three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers.

I. The Framework Core is a set of cybersecurity activities and references that are common across critical infrastructure sectors organized around particular outcomes. The Framework Core consists of five Functions that can provide a high-level, strategic view of an organization's management of cybersecurity risk. The Framework Core then identifies underlying key Categories and Subcategories for each of these Functions, and matches them with Informative References such as existing standards, guidelines, and practices for each Subcategory.

II. A Framework Profile ("Profile") represents the outcomes that a particular system or organization has achieved, or is expected to achieve, as specified in the Framework Categories and Subcategories. Profiles are also used to identify opportunities for improving cybersecurity by comparing a "Current" Profile with a "Target" Profile.

III. Framework Implementation Tiers ("Tiers") describe how cybersecurity risk is managed by an organization. The Tier selection process considers an organization's current risk management practices, threat environment, legal and regulatory requirements, business/mission objectives, and organizational constraints. The Tiers characterize an organization's practices over a range, progressing from informal, reactive implementations to approaches that are agile and risk-informed. As a result, the preliminary Cybersecurity Framework provides a common language and mechanism for critical infrastructure organizations to: 1) describe their current cybersecurity posture; 2) describe their target state for cybersecurity; 3) identify and prioritize opportunities for improvement within the context of risk management; 4) assess progress toward the target state; 5) foster communications among internal and external stakeholders; and 6) identify and mitigate impacts of information security measures or controls to protect individual privacy and civil liberties.

Section 7(c) of the E.O. requires the Cybersecurity Framework to include methodologies to identify and mitigate impacts of the Cybersecurity Framework and associated information security measures or controls on business confidentiality, and to protect individual privacy and civil liberties. These methodologies comprise a "Privacy Methodology" section of the Cybersecurity Framework. The Privacy Methodology section is being designed to highlight privacy and civil liberties considerations and risks that organizations should be aware of when using cybersecurity measures or controls. As organizations review and select relevant categories from the Framework Core, they will review the corresponding category section in the Privacy Methodology. An assessment of the privacy and civil liberties risks associated with use of the Cybersecurity Framework and its Privacy Methodology section will be completed upon NIST release of a final Cybersecurity Framework for comment in February 2014.

This document sets out findings and recommendations, resulting from the assessment of privacy and IT security controls implemented to protect the contractor support and conference/workshop registration related PII collected as part of Cybersecurity Framework development activities against the FIPPs.

3.0 Privacy and Civil Liberties Risks/Impacts

The level of risk presented by the NIST collection and processing of support contractor and conference/workshop registration related PII are Low and in adherence with FIPPs.

These information collection and processing efforts included the following: 1) entering support contractor PII into the NIST Associates Information System (NAIS), 2) entering conference attendee PII (i.e. name, company, and email address) into the NIST Conference Registration System (CRS), and 3) storing comments received from the public via email or websites on NIST computers which may include PII.

FISMA required IT security controls are confirmed for each NIST system used to process the PII, including an approved and published Privacy Impact Assessment (PIA) which is updated annually as part of the Assessment and Authorization (A&A) risk management framework and continuous monitoring process. The NIST PIAs are on the web at http://nist.gov/director/oism/policies.cfm. All are reviewed and approved using the DOC PIA process, and included as part of the package used by the authorizing official to make the annual reauthorization decision.

4.0 Fair Information Practice Principles (FIPPs) Analysis

This section provides an analysis of the NIST's Cybersecurity Framework development activities involving PII collection and processing against the FIPPs.

4.1.1 Transparency

Transparency objectives were fully met with NIST creation of the Cybersecurity Framework public website at http://www.nist.gov/itl/cyberframework.cfm. This website provides access to all supporting documents, links to current and previous workshops/events, framework development, the RFIs and Notice of Inquiry (NOI).

The NIST engaged the public for comments using the RFI process which required publication in the Federal Register for each round of comments. The latest 45-day public comment period opened on October 29, 2013 for the preliminary Framework in the Federal Register. Complete details about the comment process and period can be found at https://www.federalregister.gov/articles/2013/10/29/2013-25566/request-for-comments-on-the-preliminary-cybersecurity-framework. All comments will be posted at http://csrc.nist.gov/cyberframework/preliminary_framework_comments.html, without change, or redaction, and commenters are reminded not to include information they do not wish to be posted (e.g., personal or business information).

The NIST additionally posts PIAs for systems used to process PII at http://nist.gov/director/oism/policies.cfm. The PIAs provide notice of the NIST information practices including the use, potential recipients, and nature of the data collected. The NIST PIAs also identify how the confidentiality, integrity and availability of the information will be maintained.

4.1.2 Individual Participation

Individual participation in the Cybersecurity Framework development process was purely voluntary. The PII collected as part of the process was limited to the conference/workshop participant's name, company name, e-mail address, and public comments which sometimes included PII. The NIST met individual participation objectives, by publishing conference/workshop registration information at each workshop. NIST also published comments collected during the public comments phase. This

afforded participants an effective mechanism for appropriate access, correction, and redress regarding the use of PII.

4.1.3 Purpose Specification

The NIST ensured that PII collected as part of Cybersecurity Framework development activities was used only for conference/workshop registration and public comment processing purposes. These purposes are specified on the Cybersecurity Framework registration and public comment website at http://www.nist.gov/itl/cyberframework.cfm.

4.1.4 Data Minimization

The NIST collected the minimum amount of PII data which was directly relevant and necessary for conference/workshop registration and public comment processing. The NIST follows documented guidelines for retention and deletion to ensure PII is retained only as long as is necessary to fulfill the specified purpose. These guidelines are captured in NIST PIAs at http://nist.gov/director/oism/policies.cfm.

4.1.5 Use Limitation

The PII collected during the development of the Cybersecurity Framework was used only for workshop registration and public comment processes, in accordance with guidance set forth on the public websites for registration and the Federal Register request for comments.

4.1.6 Data Quality and Integrity

Any information collected during the Cybersecurity Framework development process was subject to correction using administrative processes in place at NIST. This includes registration information. If an individual or business found that their information was incorrect, they were able to notify the workshop's on-site administrator of the required updates, and the administrator applied the requested changes to ensure accuracy and data quality. Changes to information collected in the comments process followed the normal Federal Register comments process for updating.

4.1.7 Security

All information collected during the Cybersecurity Framework development process was stored in a FISMA certified environment. This included support contractor, conference/workshop registration, and public comments information. During the collection process, PII was obtained using approved encryption processes for data transmission. All information processing systems are accredited using the current risk management framework process.

4.1.8 Accountability and Auditing

All NIST systems used to support Cybersecurity Framework development were FISMA certified. This ensured compliance with departmental IT security and privacy policy and guidance. The combination of data minimization practices and the administrative review controls ensure data integrity and accountability.

5.0 Civil Liberties Considerations

No civil liberties risks/impacts were presented by Cybersecurity Framework development activities; thus none were assessed.

6.0 Conclusions and Recommendations

The level of risk presented by the NIST's collection and processing of support contractor and conference/workshop registration related PII are Low and in adherence with FIPPs, including that presented by the storage of any PII submitted voluntarily during a public comment period. The NIST must continue to ensure appropriate privacy and civil liberties protections are incorporated and maintained in all Cybersecurity Framework development activities.

An assessment of the privacy and civil liberties risks associated with the Privacy Methodology section of the Cybersecurity Framework must be conducted upon NIST's release of the final Cybersecurity Framework for comment. This assessment, along with the assessment of any remaining E.O. directed DOC activities involving privacy and civil liberties risks will be submitted to DHS for publication in the 2014 Compiled E.O. SAOP/CL Public Report.

U.S. Department of Commerce
E.O. 13636 Privacy and Civil Liberties (CL) Assessment Report

Published December 2013

PART VI

DEPARTMENT OF HEALTH AND HUMAN SERVICES

DEPARTMENT OF HEALTH & HUMAN SERVICES

Office of the Secretary

Office of the Chief Information Officer
Assistant Secretary for Administration
Washington, D.C. 20201

December 6, 2013

Honorable Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security
Washington, D.C. 20528

Honorable Megan H. Mack
Officer for Civil Rights and Civil Liberties
Department of Homeland Security
Washington, D.C. 20528

Dear Ms. Neuman and Ms. Mack:

The Department of Health and Human Services transmits the first report of its Assessment under section 5 of Executive Order 13636. We understand that in two to three weeks this draft will go to the National Security Staff for an IPC review, and that there will be an LRM review process through OMB before release on March 23.

If you have questions or need further information, please contact Matthew Olsen of my staff at 202-690-6162, matthew.olsen@hhs.gov, or Maya Bernstein in the Office of the Assistant Secretary for Planning and Evaluation at 202-690-7100, maya.bernstein@hhs.gov.

Sincerely,

Frank Baitman
Chief Information Officer and
Senior Agency Official for Privacy

Executive Order 13636
Section 5 Assessment
Department of Health & Human Services

Executive Order (EO) 13636, "Improving Critical Infrastructure Cybersecurity," establishes national policy on cybersecurity designed to improve information sharing and to develop and implement risk-based cybersecurity standards across major economic sectors. The EO also calls for development of a Cybersecurity Framework "to help owners and operators of critical infrastructure identify, assess, and manage cyber risk." In a related document,[1] the Department of Health and Human Services (HHS, the Department) is designated as Sector-Specific Agency for the Healthcare and Public Health Sector, and, jointly with the Department of Agriculture, HHS is Co-Sector-Specific Agency for the Food and Agriculture Sector.

In these capacities, HHS is responsible for working with private sector Healthcare and Public Health Sector organizations and with private sector owners/operators or associations within the Food and Agriculture Sector on voluntary initiatives to improve the security and resilience of physical and cyber critical infrastructure. Section 5 of the EO requires agencies to

> coordinate their activities under this order with their senior agency officials for privacy and civil liberties and ensure that privacy and civil liberties protections are incorporated into such activities. Such protections shall be based upon the Fair Information Practice Principles and other privacy and civil liberties policies, principles, and frameworks as they apply to each agency's activities.[2]

In addition, the Department is required to conduct assessments of its activities under EO 13636 and provide those assessments to DHS for consideration and inclusion in an annual government-wide report.

The activities HHS has undertaken to implement EO 13636 are not expected to have any significant privacy or civil liberties impacts that necessitate further assessment under EO 13636. The following report, submitted by the Chief Information Officer (CIO), who also serves as the Senior Agency Official for Privacy, on behalf of HHS, summarizes HHS' usual procedures for assessing privacy and civil liberties issues, and HHS' participation in activities implementing EO 13636 to date.

HHS Privacy Program

As the US Government's principal agency for protecting the health of all Americans and providing essential human services, especially for those who are least able to help themselves,

[1] Presidential Policy Directive 21, Critical Infrastructure Security and Resilience, Feb. 12, 2013 (PPD-21), *available at* <http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>.

[2] Exec. Order No. 13636, 78 Fed. Reg. 11739, 11740 (Feb. 12, 2013), *available at* <http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>.

HHS collects, assesses, and uses significant amounts of data every day. HHS is committed to protecting the security of all data used by the Department throughout its lifecycle, and is especially sensitive to the risks associated with the collection, use, storage, and sharing of personally identifiable information (PII) including protected health information (PHI) under the Health Insurance Portability and Accountability Act. HHS must not only protect the information entrusted to us, but ensure that individuals are able to participate in decisions about the collection, use and sharing of PII about themselves within HHS systems when participation is appropriate. In addition, HHS leverages technologies that require sensitivity to privacy implications even though HHS may not collect PII through these technologies. HHS's regulatory activities implicate privacy concerns for members of the public in almost all of its programs. When regulated parties collect information about individuals; when they implement technologies or programs that may have an impact on individual privacy; or when required to comply with the HIPAA Privacy and Security Rules, the Department has an obligation to identify, analyze, and mitigate these concerns.

As we expand the number and types of data collected, accelerate the adoption of new technologies, and increase regulatory complexity in response to new legislative mandates, risks to individual privacy may increase. Therefore, HHS focuses on incorporating risk management into every phase of system and program development. Risk management improves compliance with privacy objectives by raising awareness among employees and leadership regarding the standards for data safety. It institutes frameworks for training, compliance assessment, and vulnerability repair. It also promotes awareness among staff of appropriate standards for collection, use, sharing, and disclosure of PII, functions that implicate privacy concerns distinct from security. Overall, risk management improves safety and security by reducing the possibility of errors in policies, behaviors, or technologies that could lead to undesirable privacy outcomes.

HHS is fully committed to protecting the personal privacy of all individuals whose data the Department touches or over which it has regulatory or administrative authority. HHS also has a responsibility to ensure that individuals are treated with fairness and respect. Therefore, HHS established a Privacy Program to ensure that, in addition to compliance with the law, principles of fairness are observed and followed by all HHS employees and contractors.

EO 13636 references the "Fair Information Practice Principles (FIPPs)" a statement regarding the appropriate collection, use, dissemination, protection, and disposition of data developed by the Department of Homeland Security in 2008. The DHS FIPPs are based on the original Code of Fair Information Practice developed in 1973 by an advisory committee to HHS's predecessor agency, the Department of Health, Education and Welfare and which formed the framework for the Privacy Act of 1974. Other privacy statutes, federal and state policy, and even international privacy laws and regulations are all based on the core values embodied in the original Code. They address privacy concerns common to all information systems that comprise identifiable information and provide a platform for identifying, assessing, and mitigating privacy risk. HHS continues to look to the Code of Fair Information Practice and more recent formulations, such as the DHS FIPPs, in performing its privacy functions.

The FIPPs must be applied whenever an HHS program or activity collects information or raises privacy concerns involving the collection of PII. In addition, the FIPPs will be applied to the

deployment of any technology or development of any proposed regulation that raises privacy risks for individuals. This is a media-neutral policy and applies to all records regardless of whether they are created or maintained on paper or in an electronic format, unless otherwise specified in the policy.

Privacy Integration

HHS divides responsibilities for privacy policy and privacy compliance among several offices, each of which has a particular role, and each of which coordinates with the others to effectuate a Department-wide response to EO 13636. A Cybersecurity Work Group, chaired by the CIO, serves to coordinate various cybersecurity activities across the Department. With respect to Executive Order 13636, the Assistant Secretary for Preparedness and Response (ASPR), the Food and Drug Administration (FDA), and the Office of the Chief Information Officer (CIO) lead the Department implementation. The Office of Security and Strategic Information (OSSI), the Assistant Secretary for Planning and Evaluation (ASPE), the Office of the National Coordinator for Health Information Technology (ONC), and the Office of the General Counsel (OGC), provide supporting roles according to their expertise in advising on cyber and kinetic threats, privacy policy, health information technology, and legal matters, respectively. These offices make up the Cybersecurity Work Group, with occasional representation from other Departmental components as needed, and meet periodically to communicate and coordinate activities regarding implementation of the Executive Order, among other activities.

HHS has reviewed all draft EO 13636 work products disseminated for interagency review and actively participates in internal discussions and working groups. In addition, HHS is represented on the Interagency Task Force (ITF) and the ITF's Assessments Working Group.

To date, the Department has not completed implementation of any new systems or programs in response to EO 13636. As HHS moves through the system development lifecycle, the Cybersecurity Work Group will play a critical role in identifying, assessing, and mitigating privacy risk in accordance with fair information practices.

HHS and Civil Liberties

HHS is generally not engaged in activities that implicate an individual's civil liberties as might be the case for a law enforcement or national security agency. The Department has extremely narrow and limited authorities regarding the ability to arrest or hold individuals in a way that would deprive them of their civil liberties. The National Institutes of Health (NIH) does have a campus police force, and the FDA has law enforcement authority to protect FDA-regulated products,[3] but in the case of an incident, these agencies generally coordinate and cooperate with other law enforcement entities external to the Department, such as local law enforcement officials or the Federal Bureau of Investigation. The Centers for Disease Control and Prevention (CDC) has public health authority to order the apprehension, detention, or conditional release, including the isolation or quarantine, of individuals arriving into the United States from a foreign

[3] FDA has regulatory authority for a variety of products—most of our nation's food supply, cosmetics, dietary supplements, human and veterinary drugs, medical devices, vaccines and other biological products, products that give off radiation, and tobacco products.

country or moving between states if it reasonably believes that such individuals are either infected with or exposed to one of nine quarantinable diseases, as defined by executive order.[4] Such legal authorities are used on a rare basis, such as when necessary to determine whether a foreign traveler may have exposed other passengers on a plane to a dangerous communicable disease, or when necessary to allow for a smooth transition to state or local public health control. CDC does not have law enforcement authority and relies on other federal agencies, in particular Customs and Border Protection and U.S. Coast Guard, or State and local law enforcement assistance, in carrying out its responsibilities when the individual in question is not compliant with public health orders.

Despite this limited authority, we are nevertheless aware of our responsibilities to analyze and mitigate the risk to constitutional liberties that any of our activities may present, and our OGC regularly participates in discussions related to the Department's EO 13636 efforts.

OGC in partnership with the Cybersecurity Working Group will inform Department executives about applicable legal authorities and limitations for proposed activities and related procedures during the program establishment and planning phases.

HHS Participation Under EO 13636

Consistent with its responsibilities as the lead for the Healthcare and Public Health Sector, and Co-lead for the Food and Agriculture Sector, HHS has engaged in a supporting role in completing several action items under EO 13636, which are detailed below.

Cybersecurity Information Sharing. HHS is currently participating in the interagency Cybersecurity Information Sharing Working Group, which is charged with developing reporting instructions and a process to disseminate reports that will facilitate an increase in the volume, timeliness, and quality of cyber threat information shared by the U.S. government with private sector entities. HHS's current participation is limited to providing review and comment on draft products developed by the Department of Homeland Security (DHS) in close coordination with Department of Justice and the Office of Director of National Intelligence, and disseminated for interagency review.

Cybersecurity Framework. The National Institute of Standards and Technology (NIST), within the Department of Commerce, has been specifically tasked by EO 13636 to lead the development of a Cybersecurity Framework that includes a set of standards, methodologies, procedures and processes to address cyber risk. The Cybersecurity Framework is being developed in an open manner with input from stakeholders in industry, academia, and government, including a public review and comment process, workshops, and other means of engagement. HHS is working with Healthcare and Public Health Sector and Food and Agriculture Sector stakeholders to encourage participation in these workshops and the Framework review process. HHS is also working with these stakeholders to develop guidance and activities to support adoption of the Framework.

[4] Exec. Order 13295, 68 Fed. Reg. 17255, Revised List of Quarantinable Communicable Diseases (Apr. 4, 2003), *as amended by* Exec. Order No. 13375, 70 Fed. Reg. 17299, Amendment to Executive Order 13295 Relating to Certain Influenza Viruses and Quarantinable Communicable Diseases (Apr. 1, 2005).

Voluntary Critical Infrastructure Cybersecurity Program. HHS is currently participating in an interagency working group that is responsible for assembling a voluntary program to support adoption of the Cybersecurity Framework by critical infrastructure owners and operators, and other entities. HHS participation thus far has been limited to attending working group meetings and providing input on basic focus areas of the voluntary program and how it should be crafted to ensure broad participation across both public and private sectors.

Identification of Critical Infrastructure at Greatest Risk. As a Sector-Specific Agency for the Health Care and Public Health Sector, and Co-Sector-Specific Agency for the Food and Agriculture Sector, HHS has participated actively in the process to identify critical infrastructure most at risk in a cybersecurity incident; these were included on a list that was submitted by DHS to the White House.

PART VII

DEPARTMENT OF TRANSPORTATION

Memorandum

U.S. Department of Transportation
Office of the Secretary
of Transportation

Subject: U.S. Department of Transportation Privacy and Civil Liberties Analysis Pursuant to Section 5 of Executive Order 13636

Date:
Reply to: C. Barrett, OCIO

From: John D. Porcari
Deputy Secretary
Office of the Secretary

Thru: Richard L. McKinney
Chief Information Officer
Office of the Chief Information Officer

To: Karen L. Neuman,
Chief Privacy Officer
U.S. Department of Homeland Security

Megan H. Mack,
Officer for Civil Rights and Civil Liberties
U.S. Department of Homeland Security

OVERVIEW

The Cybersecurity Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," (EO 13636) establishes national policy on cybersecurity by facilitating partnership with owners and operators of critical infrastructure to improve information sharing and to develop and implement risk-based cybersecurity standards.

Section 5 of EO 13636 requires agencies to "coordinate their activities under this order with their senior agency officials for privacy and civil liberties and ensure that privacy and civil liberties protections are incorporated into such activities. Such protections shall be based upon the Fair Information Practice Principles and other privacy and civil liberties policies, principles, and frameworks as they apply to each agency's activities."[1]

[1] http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

In conjunction with EO 13636, the President signed Presidential Policy Directive-21: Critical Infrastructure Security and Resilience[2] (PPD-21). The directive recognizes the complexity of managing and protecting 16 distinct but interdependent critical infrastructure sectors throughout the nation and, subsequently, designates Sector-Specific Agencies with institutional knowledge and specialized expertise to advise and collaborate on the implementation of the directive. As the co-chair of the Transportation Sector, the U.S. Department of Transportation (DOT) works with the U.S. Department of Homeland Security (DHS) to strengthen the security and resilience of critical infrastructure and serve as a day-to-day Federal interface for prioritization and coordination of sector-specific activities.

The Department is required to conduct annual assessments of its activities under EO 13636 and provide those assessments to the DHS for consideration and inclusion in a government-wide report. While DOT has not implemented any programs or systems under EO 13636 during the reporting period, I am submitting this report on behalf of DOT to include DOT's supporting role in completing several action items under EO 13636.

DOT Privacy Program

In its mission to ensure a fast, safe, efficient, accessible and convenient transportation system that meets our vital national interests and enhances the quality of life, DOT collects, assesses, and uses significant amounts of data every day. The Department is committed to protecting the safety of all data used in the system development lifecycle, but is especially aware of the risks associated with the collection, use, storage, and sharing of personally identifiable information (PII). It is vitally important that DOT not only protect this information but ensure that individuals are able to appropriately control the collection, use and sharing of their own PII within DOT systems. In addition, DOT leverages technology that raises privacy concerns even though DOT may not collect PII through these technologies. The DOT's regulatory activities may also create privacy concerns for members of the public by requiring regulated parties to collect information on individuals or implement technologies or programs impacting individual privacy. The Department has an obligation to identify, analyze, and mitigate these concerns.

With increased data collection, technology acceleration, and regulatory complexity comes increased privacy risk, which is why DOT focuses on incorporating proactive risk management into every stage of system and program development. Risk management improves compliance with privacy objectives by raising awareness among employees and leadership regarding the standards for data safety. It institutes frameworks for training, compliance assessment, and vulnerability repair. Overall, it improves safety and security by reducing the possibility of errors in behaviors, technologies, and other business entities that could lead to undesirable privacy outcomes including, but not limited to, the loss of public support, unauthorized use or access to PII, and increased oversight.

The Department is fully committed to protecting the personal privacy of all individuals. Certain privacy protections are stated in law; however, DOT recognizes that compliance with the letter of the law is not enough. The Department also has a responsibility to ensure that individuals are

[2] http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

treated with fairness and respect; therefore, it has established a Privacy Program to ensure that in addition to compliance with the law, DOT's *Privacy Principles* are integral to every policy decision and are observed and followed by all DOT employees and contractors.

The Fair Information Practice Principles (FIPPs)

The Fair Information Practice Principles (FIPPs) are a widely accepted framework that are at the core of the Privacy Act of 1974 and are mirrored in other statutes and Federal policy and guidance. The FIPPs cover a wide area of common privacy concerns and provide a common platform for identifying, assessing, and mitigating privacy risk. The DOT Privacy Office (PO), therefore, has adopted the FIPPs as its privacy policy framework and seeks to apply them to the full breadth and diversity of DOT programs and activities.

The FIPPs provide the foundation of all DOT privacy policy development and implementation. The FIPPs must be applied whenever a DOT program or activity collects information or raises privacy concerns involving the collection of PII. In addition, the FIPPs will be applied to the deployment of any technology or development of any proposed regulation that raises privacy risks for individuals. This is a media-neutral policy and applies to all records regardless of whether they are created and/or maintained on paper or in an electronic format, unless otherwise specified in policy. To the extent practical and permitted by law, DOT extends its application of the FIPPs to all individuals living or deceased and to all individuals regardless of legal status.

Privacy Integration

The DOT PO has been a key component in DOT's efforts in response to EO 13636 and was among the first offices assigned to support the program. The DOT PO has provided reviews of all draft work products disseminated for interagency review and actively participates in internal discussions and working groups. In addition, the DOT PO participates in the Interagency Task Force (ITF) Assessments Working Group. To date, DOT has not implemented any new systems or programs in response to EO 13636. As DOT moves through the system development lifecycle the DOT Privacy Office will play a critical role in identifying, assessing, and mitigating privacy risk in accordance with the DOT FIPPs.

Civil Liberties

As previously stated, DOT has not implemented any programs or systems under EO 13636. However, DOT is aware of its responsibilities to analyze and ameliorate any activities or programs that may implicate the Constitutional rights of individuals. With this in mind, the Office of General Counsel (OGC) regularly participates in internal discussions related to DOT's participation in various EO 13636 related efforts. The OGC, in partnership with the DOT Privacy Program, ensures that DOT executives understand applicable legal authorities and limitations for proposed activities and related procedures during the program establishment and planning phases.

DOT PARTICIPATION UNDER EO 13636

Consistent with its responsibilities as a co-lead for the Transportation Sector, DOT has engaged in a supporting role in completing several action items under EO 13636, which are detailed below.

Cybersecurity Information Sharing. The DOT is currently participating in the Cybersecurity Information Sharing Working Group, which is charged with developing reporting instructions and a process to disseminate reports that will facilitate an increase in the volume, timeliness, and quality of cyber threat information shared by the U.S. government with private sector entities. DOT's current participation is limited to providing review and comment on draft products developed by DHS in close coordination with the Department of Justice and the Office of Director of National Intelligence, and disseminated for interagency review.

Development of Cybersecurity Framework. The National Institute of Standards and Technology (NIST), within the Department of Commerce, has been specifically tasked by EO 13636 to lead the development of a Cybersecurity Framework that includes a set of standards, methodologies, procedures and processes to address cyber risk. The Department has been participating as part of a working group tasked with creating overarching performance goals to accompany the Cybersecurity Framework. These goals outline what both the public and private sectors are encouraged to adopt as an end-state to secure their cyber systems and maintain availability of essential services.

The Cybersecurity Framework is being developed in an open manner with input from stakeholders in industry, academia, and government, including a public review and comment process, workshops, and other means of engagement. As a co-chair of Transportation-related sectors, DOT has also been asked to contact transportation stakeholders and encourage participation in the targeted workshops, specifically to offer substantive input on the level of guidance, presentation of the Cybersecurity Framework, implementation, and governance.

Voluntary Critical Infrastructure Cybersecurity Program. The Department is currently participating in a working group that is responsible for assembling a voluntary program to support adoption of the Cybersecurity Framework by critical infrastructure owners/operators and other entities. The DOT's participation thus far has been limited to attending working group meetings and providing input on basic focus areas of the voluntary program and how it should be crafted to ensure broad participation across both public and private sectors.

Identification of Critical Infrastructure at Risk. As a co-chair of Transportation-related sectors, DOT has been heavily involved in the process to identify critical infrastructure most at risk in a cybersecurity incident, which resulted in a classified list that was submitted to the White House on June 12, 2013. The DHS, as the primary lead on a working group formed to develop this critical cyber-dependent infrastructure list, lead the facilitation of engagement sessions with industry and government representatives from five transportation sector modes: Aviation, Maritime, Mass Transit, Pipeline and Rail. Subject matter experts from each of the DOT Operating Administrations participated in all sessions to provide a general understanding of the systems, services, and networks that composed each transportation mode. Participating DOT

representatives also provided information to the working group about whether a cybersecurity incident could result in incapacitation of an asset or function, and whether any of the transportation assets classified under the specific mode would meet the criteria for inclusion on the list of highly cyber-dependent critical infrastructure. Additionally, DOT reviewed and commented on the transportation-related inclusions to this list.

cc: Operating Administration Administrators

PART VIII

DEPARTMENT OF ENERGY

Department of Energy
Washington, DC 20585

December 5, 2013

MEMORANDUM FOR: KAREN L. NEUMAN
DHS CHIEF PRIVACY OFFICER

MEGAN H. MACK
DHS OFFICER FOR CIVIL RIGHTS AND CIVIL LIBERTIES

FROM: JERRY G. HANLEY
CHIEF PRIVACY OFFICER

SUBJECT: Executive Order 13636, Section 5, Privacy and Civil Liberties Assessment

Pursuant to the subject Order, attached please find the Department's draft Privacy and Civil Liberties Assessment that was conducted based upon the Fair Information Practice Principles and related privacy policies and procedures that apply to the Department.

If you have any questions concerning the assessment, please contact me on 202-586-0483.

Attachment

Department of Energy

Privacy and Civil Liberties Assessment

Pursuant to

Section 5 of Executive Order 13636, Improving Critical Infrastructure Cybersecurity

I. Purpose

This assessment addresses policies and procedures and establishes responsibilities for ensuring that privacy and civil liberties are incorporated into sector specific activities of the Department as required by Section 5 of Executive Order 13636 (the E.O.) and implementation guidance issued by the National Security Staff (NSS). Specifically, Section 5 of the E.O. requires department privacy officials to incorporate privacy and civil liberties protections into sector activities, and to conduct assessments of those activities, based on the Fair Information Practice Principles (FIPPs) and related policies, principles and frameworks.

II. Scope

This assessment applies to all Department of Energy (DOE) activities related to the energy sector as defined in Presidential Policy Directive -21 of February 12, 2013 (Critical Infrastructure Security and Resilience). DOE has instituted policies whereby privacy protections are applied to all activities associated with personal information that is collected, used, maintained, and/or disseminated in connection with a departmental function. As a result, these policies also apply to activities associated with the energy sector specific activities. [1]

These policies incorporates both statutory and regulatory standards with which DOE is required to comply and best practices that DOE has determined are essential to providing

[1] DOE O 206.1, *Department of Energy Privacy Program*; 10 CFR 1008. *Privacy Act Implementation*

adequate privacy and civil liberties protections to information that the Department collects and shares in the performance of its mission.

Departmental Elements may issue additional policies, procedures, and guidance, provided they comply with existing laws, regulations, and Departmental policies and procedures.

III. Goal

It is the goal of this assessment to facilitate the collection and use of information to achieve the lawful purpose(s) for which the data were collected and to meet DOE's responsibilities in delivering efficient, accessible, and convenient systems and services while protecting the privacy, civil rights, and civil liberties of U.S. citizens and lawful permanent residents.

IV. Definitions and Authorities

See Appendix A – Definitions and Appendix B – Authorities.

V. Policy

DOE maintains high standards for privacy protections, including the protection of information collected and shared with other sector specific agencies. All Departmental organizations shall comply with applicable laws, regulations, Executive Orders, Office of Management and Budget (OMB) requirements and guidance, and other pertinent policies and guidelines relating to privacy protections, including NSS privacy guidelines that are applicable to energy sector specific activities. This assessment is based on the following foundational principles of FIPPS for identifying and evaluating privacy risks.

A. Collection (Acquisition and Access)

Personally Identifiable Information (PII) shall be collected lawfully and fairly, and shall be limited to that data which is required to complete transaction(s) relevant to the Department's sector specific mission. DOE has adopted internal policies and procedures requiring it to only seek or retain PII that is legally permissible for it to seek or retain under applicable laws, regulations, policies, and Executive Orders. All information collected will only be used for the purpose for which it was collected. Prior to beginning a new or modified information collection effort, all Departmental Elements shall assess information collection practices to verify that:

1. Data collection is limited to that which is essential to DOE's mission.

2. DOE has received approval from OMB for the collection, in compliance with the Paperwork Reduction Act, if applicable.[2]
3. To the greatest extent possible, information is collected directly from the individual about whom it is collected.
4. The Privacy Office has been notified of the information collection.
5. A Privacy Impact Assessment (PIA) has been conducted consistent with DOE O 206.1.

B. Transparency & Notice

Departmental Elements and information system owners ("system owners") participating in energy sector activities will establish notice mechanisms for communicating information regarding the nature of sector specific activities that could affect privacy. These notice mechanisms will ensure the general public is aware of the collection, use, and sharing of information consistent with applicable legal and DOE policy requirements. Notice will, to the extent feasible, provide information to the public describing all PII collection, use, sharing and maintenance, and that the collection is subject to specific information privacy and civil rights statutory and regulatory requirements.

C. Use Limitation

PII collected by DOE may only be used for those purposes stated in the notice given to the individual or authorized by law, including a system of records notice (SORN). Prior to using a record, system owners, in consultation with the Chief Privacy Officer shall verify that:

1. The intended activity is listed as a routine use in the applicable SORN published in the Federal Register (if a Privacy Act system of records). If a routine use needs to be changed or added, modifications are published in the Federal Register 30 days prior to those changes going into effect and allow for interested persons to submit comments.
2. If the use is part of a computer matching program, that program meets all requirements listed in the Computer Matching Act.
3. The individual has provided consent to the use of the record for that purpose if the use is for a purpose other than that for which the record was collected, unless the use is otherwise authorized by law.
4. Information available from and shared by DOE will only be used in a manner that is consistent with the authorized purpose of the collection.

D. Data Quality and Integrity

[2] Information on obtaining approval from OMB for forms collecting personal information can be found at https://www.directives.doe.gov/pdfs/doe/doetext/neword/206/o2061.pdf.

DOE will use and share PII about persons contained in agency systems only if it is authorized to do so and the information is reasonably considered accurate and appropriate for a documented purpose and to protect the integrity of the data.

The Department takes a number of steps to ensure data quality and integrity:

- DOE will investigate in a timely manner alleged errors and deficiencies in its information and correct, delete, or refrain from using personal information found to be erroneous or deficient.
- Upon receiving information from any source that DOE determines may be inaccurate, DOE will notify in writing the contributing entity.
- The Department also has redress mechanisms in place whereby, subject to applicable and appropriate exemptions claimed for DOE systems of records under the Privacy Act, individuals may request correction of their data.
- When merging PII about an individual from two or more sources, DOE will ensure that the information is about the same individual**.**
- The Department retains personal information only so long as it is relevant and timely for appropriate use by the Department, and updates, deletes, or refrains from using personal information that is outdated or otherwise irrelevant for such use.

E. Sharing and Dissemination

DOE ensures personal information that the agency makes available in support of agency sector specific activities has been lawfully obtained by the agency and may be lawfully shared and disseminated to other agencies. Departmental Elements must:

1. Only share information in mixed systems consistent with Information Sharing Environment (ISE) policies.
2. Review personal information to be shared before it is made available to the ISE.
3. Put in place a mechanism to enable participants with whom it shares and its own employees to determine the nature and sensitivity of the personal information, so it can be handled in accordance with applicable legal requirements.
4. Disseminate DOE employee personal information in accordance with appropriate security controls such as encryption and privacy protections as required by law (e.g., the Privacy Act).

F. Access and Correction

In order to ensure the accuracy of personal information records used by DOE, individuals who submit information are afforded access to their records and have the ability to contest information they believe to be incorrect or incomplete about themselves. Individuals seeking access to any record containing information that is part of a DOE system of records, or seeking to contest the accuracy of its content, may submit a request to do so to DOE.

1. The Chief Privacy Officer is responsible for defining, documenting and implementing policies for access to and correction of all classes of personal information records. Each DOE element shall determine the extent of access and correction that will be provided for non-Privacy Act records.
2. Procedures have been developed at the Departmental level that document the process for receiving and responding to requests for access and correction of records. Departmental Elements may develop their own procedures, provided they comply with all applicable DOE policies, laws, and OMB requirements.

G. Redress

If an individual has complaints or objections to the accuracy or completeness of personal information acquired, accessed, stored, or shared by DOE through sector agency activities that has resulted in specific, demonstrable harm to such individual, and to which the individual has no right of access, DOE will inform the individual of the procedure for submitting and resolving complaints or requests for correction.

Complaints and requests for corrections will be received by the Chief Privacy Officer or designated representative per the procedures contained in 10 CFR 1008.

The Chief Privacy Officer will acknowledge the complaint and state that it will be reviewed. The Chief Privacy Officer, however, will not confirm the existence or nonexistence of the information that is exempt from disclosure.

If the information complained of is held by DOE and may be shared, but did not originate with DOE, the Chief Privacy Officer will notify the originating agency within 10 days, in writing and will assist the originating agency upon request in correcting any identified data/record deficiencies, updating or purging the information, or verifying that the record is accurate. Any protected information originating with DOE will be reviewed and corrected in, updated, or purged from DOE data/records if it is determined to be erroneous, to include incorrectly merged information, or to be out of date. A record will be kept by the DOE of all complaints or requests for corrections and the resulting action in response to the complaint.

H. Security

DOE shall provide adequate and effective security protection for all PII to ensure protection from unauthorized access, use, modification, or destruction.[3] Each Department DOE Element shall develop policies and procedures to implement the following protections for systems that store personal information:

1. Administrative, technical, and physical safeguards are in place to protect the security and confidentiality of personal information.

[3] Departmental security policies are addressed in Department of Energy Policy 205.1B, *Departmental Cyber Security Management Policy*, and at https://www.directives.doe.gov/pdfs/doe/doetext/neword/205/p2051.pdf .

2. All protections for personal information and other sensitive information comply with the Federal Information Security Management Act of 2002 (FISMA), OMB Circular A-130, Appendix III, applicable NIST security guidance and Departmental security policies and procedures.
3. Records are securely retained and timely destroyed, consistent with approved records retention and disposition schedules.
4. Security protection shall be commensurate with the risk level and magnitude of harm the DOE and/or the record subject would face in the event of a data security breach.
5. External, authorized recipients of the DOE personal information demonstrate compliance with FISMA.
6. The DOE has implemented encryption, two-factor authentication, and PII identification and tracking software, and will consider, as appropriate, other privacy enhancing technologies.
7. Additional information security requirements are defined in information sharing access agreements.

I. Accountability, Enforcement, and Audit

In order to ensure the accountability and protection of personal information, the DOE employs the following enforcement and audit procedures:

1. DOE requires that all of its personnel report and appropriate personnel investigate and respond to violations of agency policies relating to PII, including taking appropriate action when violations are discovered.

2. DOE requires that all of its personnel cooperate with audits and reviews by officials with responsibility for providing oversight.

3. DOE has designated its Chief Privacy Officer as its official to receive reports regarding alleged errors in data that originates from the Department.

4. DOE has established review and audit mechanisms to enable appropriate officials to verify that the Department and its personnel are complying with applicable privacy policies and guidelines.

J. Training

The DOE Chief Privacy Officer shall provide training to DOE personnel (i.e., employees, detailees, assignees, and contractors) and others authorized to have access to personal information regarding DOE requirements and policies for collection, use, disclosure, and protection of personal information and, as appropriate, for reporting violations of agency privacy protection policies. Awareness is the primary goal of the DOE privacy training program. Each Departmental Element shall be responsible for implementing such a program.

1. The following authorities require DOE personnel training:
    a. Subsection (e)(9) of the Privacy Act of 1974, which requires employee training on the requirements of the Privacy Act.
    b. OMB Memorandum M-01-05 *Guidance on Inter-Agency Sharing of Personal Data - Protecting Personal Privacy* reiterates training required by the Privacy Act and emphasizes the need to communicate accountability and penalties under the law.
    c. OMB Memorandum M-05-08 *Designation of Senior Agency Officials for Privacy* requires training for employees and contractors regarding information privacy laws, regulations, policies, and procedures governing the agency's handling of personal information.
    d. Section 522 (a)(8) of the 2005 Omnibus Spending Bill for Transportation and Treasury requires training and educating employees on privacy and data protection policies to promote awareness and compliance.
2. Departmental guidance and content have been developed for use by all DOE federal and contractor employees; however, Department Elements may develop local training to augment the Departmental training, provided the local training is consistent with legal and regulatory requirements.
3. Training shall include, at a minimum, the following:
    a. Appropriate use and sharing of records covered by the Privacy Act;
    b. Criminal and civil penalties for violating the Privacy Act;
    c. Accountability for non-compliance with DOE policies;
    d. Departmental policies and procedures; and
    e. Any Departmental Element's policies and procedures, as they relate to personal information that may be shared in the ISE.
4. Training shall be provided to all employees and contractors who have or may have access to personal information or develop, manage, or maintain information systems that process and store personal information, whether employee or contractor.

K. Awareness

DOE will take steps to facilitate appropriate public awareness of its policies and procedures for implementing these Guidelines and will make this policy publicly available on request and on its web site.

L. Required Procedures

DOE has developed Departmental procedures to comply with legal and regulatory requirements. Departmental Elements may customize the Departmental procedures or develop their own, as needed, to meet their local needs, provided they are consistent with all applicable legal and regulatory requirements.

1. The following procedures are required by the Privacy Act of 1974:
    a. Procedures to respond to individual requests to access records;

b. Procedures for disclosing records, including special procedures for sensitive records;
c. Procedures for reviewing and responding to requests to make changes to a record, including how to determine approval;
d. Procedures for monitoring recipient agencies in computer matching agreements for adequate security safeguards to protect personal information records; and
e. Procedures for the timely destruction of records received from other agencies as part of a computer matching agreement.

2. Departmental Elements must review annually the systems of records subject to their responsibility to ensure compliance with the requirements of the Privacy Act.

M. Assessment of Policies and Update of Privacy Policy

DOE will continually seek to identify and assess evolving laws, policies, and procedures applicable to privacy and civil liberties and DOE will make available or access of all such laws, Executive Orders, policies and procedures, and will comply with any legal restrictions applicable to such information. This may require updating this assessment as necessary to respond to evolving laws, policies and procedures.

VI. Responsibilities

A. DOE personnel are responsible for:

1. Complying fully with the Privacy Act of 1974 and other data protection laws referenced in this policy.
2. Reviewing and signing a copy of this policy to acknowledge that they received, reviewed and understood its contents.
3. Contacting their DOE element or Departmental Privacy Officer prior to beginning new collections or uses of PII to determine if a system of records notice and/or PIA needs to be written.
4. Providing adequate security protection and confidentiality for both hard copy and electronic PII in their custody and use.
5. Attending Privacy Act and Privacy and Civil Liberties training provided by their DOE element and completing any tests or attendance verification requested as part of the training.

B. Each System Owner, in consultation with the Privacy Officer for the DOE Element is responsible for identifying data holdings that contain PII about other persons contained in mixed systems. Once identified, system owners are further responsible for ensuring that information is made available to the ISE in accordance with this assessment.

Appendix A – Definitions

Senior Agency Official for Privacy/Chief Privacy Officer, as defined by OMB Memorandum 05-07, is the senior official who has been identified to OMB by each Department as having overall responsibility for information privacy issues and for overseeing the implementation and management of the DOE Privacy Program. The CPO is responsible for ensuring that protections are implemented as appropriate through efforts such as training, business process changes, and system designs. DOE has designated the Chief Privacy Officer for this role.

Computer Matching Program is a computerized comparison of two or more automated systems of records, or a system of records with non-Federal records, with the purpose of establishing or verifying the eligibility of, or continuing compliance with statutory and regulatory requirements by, applicants for, recipients or beneficiaries of, participants in, or providers of, services with respect to cash or in-kind assistance or payments under Federal benefit programs, or recouping payments or delinquent debts under such Federal benefit programs or two or more automated Federal personnel or payroll systems of records or a system of Federal personnel or payroll records with non-Federal records.

Departmental Chief Information Officer (CIO) is the senior management official responsible for the DOE Privacy Policy Program.

Departmental Elements are the multiple organizational components and bureaus of the DOE. (https://www.directives.doe.gov/pdfs/reftools/org-list.pdf).

Individual is a citizen of the United States or an alien lawfully admitted for permanent residence.

Information Sharing Environment (ISE) is an approach to the sharing of information related to terrorism that is being implemented through a combination of policies, procedures, and technologies designed to facilitate the sharing of critical information by all relevant entities. The ISE serves the dual imperatives of enhanced information sharing to combat terrorism and protecting the information privacy and other legal rights of Americans in the course of increased information access and collaboration. The ISE is being developed by bringing together, aligning, and building upon existing information sharing policies and business processes and technologies (systems), and by promoting a culture of information sharing through greater collaboration. It is being developed pursuant to Section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004, as amended by the Implementing Recommendations of the 9/11 Commission Act of 2007 (IRTPA) and Executive Order 13388, entitled "Further Strengthening the Sharing of Terrorism Information to Protect Americans."

Information System Owner is a Federal manager who is responsible for planning, directing, and managing resources for an operational information system.

Personally Identifiable Information (PII) is any information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means, including both physical and online contact information.

Personal Information is information about DOE employees, detailees, and assignees that is collected on DOE and Office of Personnel Management standard forms.

Privacy Impact Assessment (PIA) is a documentation process that identifies and assesses security and privacy risks and mitigation efforts when planning, developing, implementing and operating information management systems and rulemakings.

Protected Information is information about U.S. citizens and lawful permanent residents that is subject to information privacy or other legal protections under the U.S. Constitution and federal laws of the United States. Protected information to be made available within the ISE includes only that which is homeland security information, law enforcement information, and terrorism information, including weapons of mass destruction information, and which terms are defined as follows:

- **Homeland Security Information**, as derived from the Homeland Security Act of 2002, Public Law 107-296, Section 892(f)(1) (codified at 6 USC § 482(f)(1)), is defined as any information possessed by a state, local, tribal, or federal agency that:
    - Relates to a threat of terrorist activity;
    - Relates to the ability to prevent, interdict, or disrupt terrorist activity;
    - Would improve the identification or investigation of a suspected terrorist or terrorist organization; or
    - Would improve the response to a terrorist act.
- **Law Enforcement Information** is defined as any information obtained by or of interest to a law enforcement agency or official that is both:
    - Related to terrorism or the security of our homeland, and
    - Relevant to a law enforcement mission, including but not limited to:
        - Information pertaining to an actual or potential criminal, civil, or administrative investigation or a foreign intelligence, counterintelligence, or counter terrorism investigation;
        - An assessment of or response to criminal threats and vulnerabilities;
        - The existence, organization, capabilities, plans, intention, vulnerabilities, means, method, or activities of individuals or groups involved or suspected of involvement in criminal or unlawful conduct or assisting or associated with criminal or unlawful conduct;
        - The existence, identification, detection, prevention, interdiction, or disruption of, or response to, criminal acts and violations of the law;

        - Identification, apprehension, prosecution, release, detention, adjudication, supervision, or rehabilitation of accused persons or criminal offenders; and
        - Victim/witness assistance.
- **Terrorism Information** is defined in IRTPA Section 1016 (codified at 6 USC § 485) as all information, whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities relating to:
    - The existence, organization, capabilities, plans, intentions, vulnerabilities, means of financial or material support, or activities of foreign or international terrorist groups or individuals, or of domestic groups or individuals involved in transnational terrorism;
    - Threats posed by such groups or individuals to the United States, United States persons, or United States interests, or to those of other nations;
    - Communications of or by such groups or individuals; or
    - Groups of individuals reasonably believed to be assisting or associated with such groups or individuals.

  The definition includes weapons of mass destruction information.
- **Weapons of Mass Destruction Information** is defined in IRTPA Section 1016 (codified at 6 USC § 485) as information that could reasonably be expected to assist in the development, proliferation, or use of a weapon of mass destruction (including a chemical, biological, radiological, or nuclear weapon) that could be used by a terrorist or terrorist organization against the United States, including information about the location of a stockpile of nuclear materials that could be exploited for use in such a weapon that could be used by a terrorist or terrorist organization against the United States.

Record, as defined by the Privacy Act of 1974, is any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, the individual's education, financial transactions, medical history, and criminal or employment history and that contains the individual's name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

Routine Use is defined in the System of Records notice as what activities, uses and disclosures may take place for the record. Routine uses must be compatible with the primary uses of the system.

Sector Specific Agency means the Federal department or agency designated under PPD-12 to be responsible for providing institutional knowledge and specialized expertise as well as leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector in the all-hazards environment.

Statistical Record is that maintained for statistical research or reporting purposes only and not used in whole or in part in making any determination about an identifiable individual.

System of Records is a group of manual or electronic records maintained by the Federal Government from which information is retrieved by the name of the individual or identifying number, symbol, or other particular assigned to the individual. The Privacy Act applies to systems of records.

Appendix B – Authorities

Executive Order 13636, Improving Critical Infrastructure Cybersecurity

Presidential Policy Directive/PPD-21, Critical Infrastructure Security and Resilience.

Intelligence Reform and Terrorism Prevention Act of 2004, *as amended by* the Implementing Recommendations of the 9/11 Commission Act of 2007 (50 U.S.C. § 402 *et seq.*)

The Privacy Act of 1974, as amended by The Computer Matching and Privacy Protection Act of 1988; 5 USC § 552a

OMB Privacy Act Implementation Guidelines and Responsibilities

OMB Final Guidance on Interpreting the Provisions of the Computer Matching and Privacy Protection Act of 1988

Health Insurance Portability and Accountability Act (HIPAA), Standards for Privacy and Security

The E-Government Act of 2002

Federal Information Security Management Act of 2002, 44 U.S.C. § 3541

OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002

OMB Circular A-130, Management of Federal Information Resources

OMB Guidance on Inter-Agency Sharing of Personal Data – Protecting Personal Privacy

DOE Privacy Act Issuances

OMB Memorandum: Designation of Senior Agency Officials for Privacy

Public Handbook for Gaining Access to DOE Information (FOIA Request)

DOE Privacy Impact Assessment Introduction

DOE Order 205.1B, DOE Cyber Security Management
https://www.directives.doe.gov/pdfs/doe/doetext/neword/205/o2051a.pdf

DOE Order 206.1, DOE Privacy Program
https://www.directives.doe.gov/pdfs/doe/doetext/neword/206/o2061.pdf

Appendix C – Acronyms

DOE	Department of Energy
FISMA	Federal Information Security Management Act of 2002
FOIA	Freedom of Information Act
ISE	Information Sharing Environment
OMB	Office of Management and Budget
PIA	Privacy Impact Assessment
PI	Protected Information
PII	Personally Identifiable Information
SORN	System of Records Notice

PART IX

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
CIVIL LIBERTIES AND PRIVACY OFFICE

December 2, 2013

Ms. Karen L. Neuman
DHS Chief Privacy Officer
U.S. Department of Homeland Security
Washington, D.C. 20528

Ms. Megan H. Mack
DHS Officer for Civil Rights and Civil Liberties
U.S. Department of Homeland Security
Washington, D.C. 20528

Dear Ms. Neuman and Ms. Mack:

Enclosed is the assessment of the activities of the Office of the Director on National Intelligence (ODNI) conducted pursuant to Executive Order 13636 (February 12, 2013), Improving Critical Infrastructure Cybersecurity. As the senior agency privacy and civil liberties official, I have assessed ODNI's activities against the Fair Information Practices Principles and other applicable privacy and civil liberties policies, principles, and frameworks, as required by Executive Order 13636.

ODNI's primary activities pursuant to Executive Order 13636 involve the Director of National Intelligence instructions to the Intelligence Community regarding the timely production of unclassified cyber products for the United States homeland that identify a specific targeted entity. As Intelligence Community Directive 209, Tearline Production and Dissemination, is the basis for those instructions, our assessment reviews that Intelligence Community Directive through the lens of applicable privacy and civil liberties protections. We have determined that the activity to which the instruction applies—production of tearlines—relies on information collected and maintained pursuant to both government-wide and IC-specific privacy and civil liberties safeguards.

This constitutes my initial assessment of ODNI's activities. Further assessments will be conducted as appropriate.

Respectfully,

Alexander W. Joel
Civil Liberties Protection Officer

Office of the Director of National Intelligence
Civil Liberties and Privacy Office
Assessment of ODNI Activities Under Executive Order 13636
December 2, 2013

I. Introduction

The President issued Executive Order (EO) 13636 (February 12, 2013), Improving Critical Infrastructure Cybersecurity, to "enhance the security and resilience of the Nation's critical infrastructure," primarily through voluntary cybersecurity information sharing programs that "increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities so that these entities may protect and defend themselves against cyber threats."[1] Because the sharing of cyber threat information may involve the sharing of identifying information, the EO imposes requirements intended to mitigate those corresponding risks to privacy and civil liberties.

Specifically, EO 13636 requires agencies to "coordinate their activities [under EO 13636] with their senior agency officials for privacy and civil liberties and ensure that privacy and civil liberties protections are incorporated into such activities. Such protections shall be based upon the Fair Information Practices Principles [FIPPs] and other privacy and civil liberties policies, principles, and frameworks as they apply to each agency's activities."[2] Senior agency privacy and civil liberties officials shall assess those activities "against [FIPPs] and other applicable privacy and civil liberties policies, principles, and frameworks"[3] and provide their assessments for inclusion in an overall assessment that the Department of Homeland Security (DHS) will prepare.[4]

This first assessment under EO 13636 has been prepared by the Civil Liberties Protection Officer of the Office of Director of National Intelligence (ODNI), who leads the ODNI's Civil Liberties and Privacy Office (CLPO). The Civil Liberties Protection Officer serves as the ODNI's senior agency official for privacy and civil liberties. Further assessments will be provided, as appropriate.

II. Scope of ODNI Activities Covered by this Assessment:

In general, senior agency privacy and civil liberties officials are expected to assess only the activities of their respective agencies.[5] EO 13636 establishes four activities required of the Director of National Intelligence (DNI):

[1] EO 13636, Section 1.
[2] EO 13636, Section 5a.
[3] EO 13636, Section 5a.
[4] EO 13636, Section 5a.
[5] EO 13636, Section 5b.

- Within 120 days, issue instructions for the Intelligence Community (IC) to ensure the timely production of unclassified cyber products to the U.S. homeland that identify a specific targeted entity.[6]

- Coordinate on the DHS and Attorney General processes that will ensure the rapid dissemination of cyber products to the U.S. homeland that identify a specific targeted entity.[7]

- Coordinate on DHS and Attorney General processes that will track the production, dissemination, and disposition of such cyber products.[8]

- Provide threat and vulnerability information and technical expertise to inform the development, by the National Institute of Standards and Technology (NIST), of the Cybersecurity Framework.[9]

This assessment does not address the second, third, and fourth requirements listed above—for which other agencies hold primary responsibility and are in the early stages of development (i.e., DHS, Department of Justice, and NIST) making it premature to assess ODNI's involvement in those endeavors. Consequently, it addresses only the implications for privacy and civil liberties of the DNI's instructions to the IC for producing unclassified cyber products that identify a specific targeted entity.[10]

III. **DNI Implementation of EO 13636**

The EO mandates that the DNI issue instructions

> *consistent with [his] . . . authorities and with the requirements of section 12(c) of this order to ensure the timely production of unclassified reports of cyber threats to the U.S. homeland that identify a specific targeted entity.*[11] *The instructions shall address the need to protect intelligence and law enforcement sources, methods, operations, and investigations.*[12]

[6] EO 13636, Section 4(a). Specifically, the DNI is required to issue instructions consistent with his "authorities." As DNI's authorities pertain to the IC, the applicability of these instructions is limited to the IC.
[7] EO 13636, Section 4(b).
[8] EO 13636, Section 4(c).
[9] EO 13636, Section 7(d).
[10] This assessment does not address the individual IC elements' implementation of those instructions.
[11] The interagency working group addressing implementation of EO 13636 has defined a "specific targeted entity" as a private sector entity, or entities, owned or operated within the United States that is known by the Federal government, through any means, to be a potential target of a specific future cyber threat or victim of an on-going or past cyber threat activity. This could include multiple private sector entities that may be targeted or similarly victimized by the same specific cyber threat. Additionally, the Federal government may establish thresholds for whether a threat is reportable through this process/system based on the level of threat severity.
[12] EO 13636, Section 5(a).

Following the approval of EO 13636, ODNI requested National Security Staff (NSS) review of Intelligence Community Directive[13] (ICD) 209 Tearline Production and Dissemination.[14] The NSS determined it satisfied the foregoing requirement for DNI issued instructions. "Tearlines" are portions of an intelligence report or product that provide the substance of a classified or controlled report without identifying sensitive sources, methods, or other operational information.[15] Because sensitive and operational information has been removed, a tearline can be broadly shared with those who have need for the intelligence but who may not have the appropriate clearance to receive the full details. Tearlines are one of the means by which the DNI ensures that intelligence reports or products prepared by the IC—including, but not limited to reports of cyber threats—are appropriately disseminated to those who have a need for that information.

Thus, ICD 209 provides instructions for the production and dissemination of tearlines—including those that identify a specific targeted entity. Consistent with EO 13636 and the Presidential Policy Directive – Critical Infrastructure Security and Resilience (PPD-21)—the products prepared pursuant to ICD 209 will be disseminated to recipients through DHS and DOJ established processes. CLPO envisions that the production and dissemination of cyber tearlines will occur in the following scenarios:

- "Signature" information[16] is found that may prevent or mitigate a cyber threat. Based on this information a tearline will be prepared for appropriate distribution notifying recipients of this signature. Typically, these tearlines will not include identifying information.

- Cyber threat information identifies a potential target of a threat. In this situation, EO 13636 envisions that this threat information will be provided to the target so that an individual/entity can defend itself from the attack. Typically, any identifying information will relate to the potential target.

Regardless of which of these two scenarios is applicable, the dissemination of cyber information is predicated on the IC determining that information within the tearline meets all dissemination requirements imposed by law and policy.

IV. **Privacy and Civil Liberties Risks/Impacts:**

The foregoing has the potential to create the following general privacy and civil liberties risks:

[13] *See* ICD 101, paragraph E.1.a., ICDs "establish policy and provide definitive direction to the IC." Developed in a collaborative manner, they are binding on the entire IC, unless otherwise specifically exempted.
[14] ICD 209, was approved by the DNI on September 7, 2012.
[15] ICD 209, paragraph D.1.
[16] A characteristic or distinctive pattern that can be searched for or that can be used in matching to previously identified attacks.

- IC elements may disseminate identifying information in tearlines beyond that relevant and necessary to understand and assess the intelligence.

- Recipients of such products will retain and use identifying information for other purposes.

V. **FIPPs Analysis of the DNI's Instructions on Producing Unclassified Cyber Products**

The FIPPs are recognized as important principles of government information policy with respect to the relationship between an entity that is collecting information about individuals and the individuals who are the subject of that information. The FIPPS reflect the policy that government information collection of personally identifying information (PII)[17] should be transparent and participatory, i.e., that individuals be informed of the use to be made of information about them, that they have a choice to provide the information or consent to its disclosure, and that they be permitted to access records about themselves and correct factual inaccuracies. These principles are pillars of the Privacy Act of 1974. As these principles are translated into binding legal requirements, certain exemptions have necessarily been recognized (e.g., for national security and law enforcement purposes).

ICD 209, by its terms, does not address the IC's collection of information from individuals; rather, it prescribes procedures for fashioning and disseminating intelligence that has already been lawfully collected by the IC in accordance with other authorities. However, to satisfy the requirement in EO 13636 that we base our assessment at least partially on the FIPPs, CLPO has used the FIPPs analysis framework as the point of departure for discussing relevant post-collection measures to protect privacy and civil liberties of those whose PII may be included in intelligence products. For instance, IC elements are required under the provisions of EO 12333 to afford extensive protections to information identifying of or concerning United States persons[18] in the use and dissemination of intelligence. Because these two frameworks are not coextensive in their focus or application, this assessment includes an analysis of the requirements of EO 12333 and its implementing policies in the FIPPs analysis, where appropriate.

a. **Transparency.** As noted, under the ICD 209 framework, CLPO envisions that IC elements will develop threat intelligence report tearlines from available intelligence. It is possible that such tearlines could include PII. Where records have been collected in the first instance by a non-intelligence agency for another purpose, subject individuals[19] would have notice of a potential intelligence use of the collected information by reference to the applicable Privacy Act system of records notice (SORN) and any associated routine uses permitting

[17] PII is defined by OMB M-07-16 as information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

[18] A "United States person" under EO 12333 is defined as a United States citizen, an alien known by the intelligence element concerned to be a permanent resident alien, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments.

[19] An "individual" under the Privacy Act is defined as a United States citizen or a lawful permanent resident.

disclosure of records in that system to an IC element. Where a subject's records have first been collected by an IC agency for an investigatory purpose, the Privacy Act permits that agency to exempt itself from disclosing its investigatory purpose if the records are classified. In those circumstances the subject would not have been apprised of the fact or purpose of the collection. Nevertheless, the Privacy Act SORNs that IC elements publish alert the public to the fact that the IC collects and/or maintains PII about citizens and permanent residents, and informs the public of the uses of the information. Thus, both the IC elements' and other government agencies' published regulations and Privacy Act notices provide visibility into the administration and use (including further dissemination) of collected PII for intelligence purposes.

In addition, IC elements are subject to EO 12333, which governs all intelligence activities. Section 2.3 of EO 12333 specifically enumerates the types (categories) of information about United States persons[20] that IC elements may collect, retain, and disseminate. Thus, Section 2.3 generally informs the public how IC elements may use and disseminate information identifying a United States person.[21]

b. **Individual Participation.** The principle of Individual Participation holds that, to the extent practical and appropriate, organizations should involve the individual from whom information is collected in the processes of collecting, maintaining, using and sharing the information, generally by obtaining consent. As noted previously, the activity governed by ICD 209 does not implicate the original receipt of information from an individual. Also as noted, when the FIPPs are implemented as legal requirements, certain exemptions are included to cover national security and law enforcement activities. Specifically, it is not possible to directly allow for individual participation and consent in national security and law enforcement matters, where such involvement could compromise sensitive operational activities. In this specific context, affording an individual the option to consent to the sharing of intelligence about him/her in a cyber threat tearline could undermine the intent of EO 13636 to protect critical infrastructure from cyber threats. Within the IC, a record subject's right of participation will generally consist of the form of access or redress that is available under applicable law (e.g., the Privacy Act) or policy, depending on the nature of the information (e.g., ISE privacy guidelines for terrorism information, or the terrorist watchlisting redress procedures). In this regard, it should be noted that CLPO has the statutory responsibility to "review and assess complaints and other information indicating possible abuses of civil liberties and privacy in the administration of [ODNI] programs and operations" and to investigate such matters, as appropriate. Thus, an individual with a concern about sharing under EO 13636 and ICD 209 could raise that concern with CLPO for review, assessment, and investigation, as appropriate.

c. **Purpose Specification.** The principle of Purpose Specification states that an organization should inform record subjects about the authority for and purpose of collecting PII in a given

[20] A "United States person" under EO 12333 is defined as a United States citizen, an alien known by the intelligence element concerned to be a permanent resident alien, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments.

[21] EO 12333, Section 2.3, specifies that the IC may collect, retain, and disseminate such information only in accordance with procedures approved by the head of the element (or the head of an agency with an IC element) and the Attorney General in consultation with the DNI. These procedures are often referred to as an element's "Attorney General Guidelines." Several IC elements' procedures are available to the public.

circumstance, as required, for example, by the Privacy Act. Again, ICD 209 does not implicate the initial collection of information from individuals and therefore tearline production under this directive is neither subject to, nor does it alter, any purpose specification policy or protocols that apply at the collection stage.

Nevertheless, general notice of the IC's authority to use and disseminate information containing PII is provided through other means:

- EO 13636 informs the public that the DNI is required to issue instructions governing the dissemination of cyber threats to the U.S. homeland that identify a specific targeted entity.

- Each IC element's authorities and mission—which govern their ability to use and disseminate PII—is delineated in United States Code and/or EO 12333, Part 1.

- The IC provides regular testimony to Congressional oversight committees regarding the use of lawfully collected information.

- The IC's use of information is subject to oversight by the Intelligence Oversight Board and Privacy and Civil Liberties Oversight Board.

d. **Minimization.** The principle of Minimization holds that an organization should only collect PII that is directly relevant and necessary to accomplish a specified purpose(s) and only retain PII for as long as is necessary to fulfill that purpose(s). Although ICD 209 does not explicitly address the minimization of PII, each IC element is subject to laws and policies that effectively implement the principle of minimization that is not altered by ICD 209. These include:

- The Privacy Act: requires federal agencies to maintain "only such information about an individual as is relevant and necessary" to accomplish a lawful purpose,[22] and incorporates NARA-prescribed retention periods for the information.

- EO 12333 and Attorney General Guidelines: require IC elements to use the least intrusive collection techniques feasible within the United States or directed against United States persons[23] and prescribe limits on content and retention of information about United States persons.

- The Federal Records Control Act: requires federal agencies to maintain and dispose of records in accordance with applicable (NARA) records retention schedules.

- The Foreign Intelligence Surveillance Act (FISA): requires IC elements engaged in electronic surveillance to follow procedures approved by the Attorney General that minimize the collection, retention and dissemination of non-relevant information concerning unconsenting United States persons, and govern the dissemination of that information.

[22] 5 U.S.C. § 552a(e)(1).
[23] EO 12333, Section 2.4.

e. **Use Limitation.** The principle of Use Limitation states that an organization should only use PII for the purposes specified in the "notice" given to individuals when the information was collected. Like the principle of individual participation, it is not possible to apply this principle in the intelligence and law enforcement context in the same way that it applies in other contexts. For example, when conducting an intelligence or law enforcement investigation, it may well not be possible to provide subjects of that investigation with written notifications, since doing so would alert them to change their conduct as necessary to carry out their plans without further detection by the government. That said, IC elements provide general notice of their uses of collected PII through their published Privacy Act SORNs and through EO 12333. ICD 209 acknowledges the existence of these limiting regimes, stating that "[t]earliness containing U.S. Person information shall be disseminated in accordance with all applicable laws, Executive Orders, and Attorney General Guidelines." In practice, this means:

- The IC element is permitted to disseminate a tearline with Privacy Act-protected PII only if the production of intelligence products was a use described in the Privacy Act SORN applicable to that type PII and the dissemination is permissible pursuant to EO 12333 and the element's Attorney General Guidelines.

- PII that is not covered by the Privacy Act is subject to dissemination in a tearline consistent with the limitations of EO 12333 and the element's Attorney General Guidelines.

In sum, the principle of use limitation applies to dissemination of PII in tearlines under ICD 209 through the operation of the Privacy Act and EO 12333.

f. **Data Quality and Integrity.** The principle of Data Quality and Integrity states that organizations should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete. The Privacy Act espouses this principle through specific requirements relating to review and verification of collected information that is retained and that is being disclosed. While an exemption from these requirements is permitted depending on the circumstances, the IC nonetheless has a mission interest in ensuring data quality for information underlying its intelligence products. To further that end, IC elements are subject to the requirements of ICD 203, Analytic Standards, directing that intelligence products "meet the highest standards of integrity and rigorous analytic thinking."[24] Ensuring the fidelity of the underlying data is a prerequisite to meeting the analytic standards. Analysts producing intelligence products are required to include a key source summary statement assessing the validity of the information.[25] Additionally, IC processes have been created to ensure that information later found to be inaccurate or incomplete is corrected. For example, fully-sourced versions of all intelligence products are retained and standards are in place for tagging information disseminated electronically,[26] so that IC elements can track IC information and, where appropriate, recall and correct any information that is discovered to be inaccurate. This correction protocol applies to intelligence that an IC element has disseminated by tearline.

[24] ICD 203, paragraph B.3.
[25] ICD 206, paragraph D.5.
[26] Id., paragraph D.6., and Intelligence Community Standard (ICS) 500-21.

g. **Security.** The principle of Security states that organizations should protect PII through appropriate safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure. This principle is embedded in a variety of requirements that apply to executive branch agencies, such as the Privacy Act, the Federal Information Security Management Act (FISMA) and other statutes, Executive Orders, and regulations governing the collection, storage, use, protection, and disclosure of PII. The protective strategies are physical, technical, and administrative in nature, and provide access controls to sensitive information, physical access controls to IC facilities, confidentiality of communications, and personnel screening.

The protection of information, including PII, from unauthorized disclosures or manipulation is fundamental to the IC mission. In addition to the government-wide mandates cited above, the DNI has established overarching security requirements which he has directed heads of individual IC elements to implement in their policies and programs.[27] These include ICD 700, Protection of National Intelligence, and ICD 502, Integrated Defense of Computer Technology.

ICD 700 establishes the basic framework for the protection of intelligence within the IC. As permitted by the DNI's policies, IC elements often establish more rigorous standards for their organizations. ICD 700 establishes the following specific requirements for protecting intelligence, including PII embedded in intelligence and intelligence products:

- Intelligence and intelligence sources must be protected from unauthorized disclosure.[28]

- Internal counterintelligence and security assets must collaborate and share data and information to protect against unauthorized disclosures of information.[29]

- Internal counterintelligence and security policies, procedures, practices, and programs must be established "to ensure the identification, protection, handling, storage, access to, and dissemination of national intelligence."[30]

- "Risk management principles must be employed to minimize the potential for unauthorized disclosure or compromise of national intelligence and intelligence sources . . . ."[31]

- All personnel with access to national intelligence must have: "[a] need for access, a favorable determination of eligibility made by an authorized adjudicative agency, and a signed non-disclosure agreement. These personnel must be continually evaluated and monitored, and regularly trained in their individual security responsibilities. They must also be advised of legal and administrative obligations and the ramifications of a failure to meet those obligations."[32]

[27] See e.g., ICD 502, paragraph D.3. and ICD 700, paragraph E.2.
[28] ICD 700, paragraph E.2.a.
[29] ICD 700, paragraph E.2.b.
[30] ICD 700, paragraph E.2.c.
[31] ICD 700, paragraph E.2.d.
[32] ICD 700, paragraph E.2.e.

- Security and counter-intelligence awareness training and education programs must be established for all IC personnel.[33]

In addition, procedures are in place to safeguard the integrated electronic network that constitutes the "IC Information Environment." Because this electronic environment is only as strong as the weakest link, the DNI, in ICD 502, directed the development of a protocol (concept of operations) for the integrated defense of community assets. This protocol provides a framework where all elements of the IC collectively engage and develop unified courses of action to defend against threats or potential threats to the IC IE, including: procedures to defend and coordinate government wide defenses of the information environment; guidelines to detect, isolate, mitigate, respond, and report incidents and spills and other vulnerabilities; and standard operating procedures for an IC wide Incident Response Center.[34] Together, these policies establish a comprehensive program for protecting information within the IC information environment.

Finally, all IC personnel are vetted prior to having access to IC information, based on each element's access criteria. At a minimum, all IC personnel must have completed background investigation, and most IC elements require that employees have an active Top Secret//Sensitive Compartment Information (TS/SCI) security clearance. Many IC elements require employees to have completed a counterintelligence or full polygraph before accessing information. Employees producing and disseminating cyber tearlines mandated by EO 13636 are subject to the same rigorous access scrutiny as all other IC personnel.

In sum, the information and intelligence that serves as the basis for any tearline under ICD 209 has benefitted from rigorous IC-wide information assurance, system security and personnel security protocols, analysts may feel confident about the integrity of the information they use for tearlines.

h. **Accountability and Auditing.** The principle of Accountability and Auditing states that organizations should be accountable for complying with the FIPPs, provide training in the protection of PII to all employees and contractors, and audit the actual use of PII to demonstrate compliance with these principles and all applicable privacy protections. As with the other principles, this principle is reflected in the Privacy Act and in OMB policy issuances, which require agencies to ensure that personnel are trained in the handling and protection of PII. These requirements ensure that personnel appreciate the sensitivity of PII and are familiar with applicable protections before being allowed access to systems maintaining such information, especially with respect to systems containing Privacy Act-protected records. Properly trained personnel ensure that PII in tearlines is properly handled and protected.

In addition, the IC has instituted requirements for accountability and auditing that further ensure the integrity of information used in preparing tearlines. Specifically, ODNI has issued minimum standards applicable to all IC elements, regarding the audit of significant events,

[33] ICD 700, paragraph E.2.f.
[34] ICD 502, paragraph 2.a.

including, but not limited to accessing, downloading, printing and exporting information.[35] Such auditing is one means of ensuring the integrity of information and intelligence used in tearlines.

VI. **Beyond the FIPPs.**

Because ICD 209 governs the IC's production and dissemination of tearlines from already-collected information (including PII), the privacy and civil liberties implications of tearline production relate more to the lawfulness of using that collected information in intelligence products. This section addresses those protections as they apply to ICD 209.

The IC's authority to retain and disseminate (specific categories of) information about US persons has the potential to directly and indirectly impact civil liberties. Limitations have been placed on IC intelligence activities to protect against encroachments on civil liberties. As discussed earlier, IC elements are subject to EO 12333 during the conduct of all intelligence activities. EO 12333 provides the basic framework for the IC protecting the privacy and civil liberties of United States persons. These include, among others, the requirement in EO 12333 that IC elements must "protect fully the legal rights of all United States persons" during the conduct of all intelligence activities, including "freedoms, civil liberties, and privacy rights guaranteed by Federal law."[36]

Further, the President has required that all activities conducted pursuant to EO 13636—including the DNI's instructions to ensure the timely production of unclassified cyber products—promote civil liberties.[37] And the DNI separately has a statutory responsibility to ensure the activities of the IC comply with the Constitution and laws of the United States during the conduct of intelligence activities.[38]

a. **First Amendment**.

The United States Constitution guarantees individuals the right to engage in protected activities, such as speech, religious expression, free assembly, press, and the right to petition government for redress of grievances. ICD 209 informs IC elements that "[t]earlines containing U.S. Person information must be disseminated in accordance with all applicable laws, Executive Orders, and Attorney General Guidelines." This requirement incorporates by reference the following limitations on the IC's use of information regarding individuals' exercise of their First Amendment rights:

- The Privacy Act prohibition on maintaining any record describing how an individual exercises his First Amendment rights unless expressly authorized by statue, consented to

[35] Intelligence Community Standard (ICS) 500-27, Appendix B.
[36] EO 12333, Part 1, Section 1.1(b).
[37] EO 13636, Section 1.
[38] NSA-47, amended, § 102A(f)(4)

by the individual involved, or unless it is relevant to an authorized law enforcement activity.[39]

- Various IC elements' AG Guidelines prohibiting action based solely on constitutionally protected activities.

- EO 12333 designation of permissible (not constitutionally sensitive) categories of information for collection, retention, and dissemination.

Thus, ICD 209, by its terms, addresses the risk that information regarding constitutionally protected activities will be used in a cyber threat tearlines.

b. **Fourth Amendment.**

The Fourth Amendment to the United States Constitution protects against unreasonable searches and seizures. In order to prevent violations, various mechanisms are in place that restricts the IC from collecting information in a manner that would violate the Fourth Amendment. These include FISA, Title III of the Omnibus Crime Control and Safe Streets Act of 1968, also known as the "Wiretap Act," Electronic Communications Privacy Act of 1986, EO 12333, and IC elements' AG Guidelines.

Additionally, case law has held that "a search and seizure that results from the sharing of information that is determined to be materially inaccurate or misleading may impact Fourth Amendment interests."[40] The potential for sharing of erroneous information through tearlines is minimized, however, by IC policies and practices recited above that address data quality, correction of errors, and analytic rigor.

c. **Fifth Amendment.** The Fifth Amendment to the United States Constitution protects against the exercise of government authority without due process of law. Due process rights could be implicated if an IC element were to share inaccurate or misleading information about an individual that results in his being deprived of a liberty interest. This concern relates to the accuracy of the information that is shared. As discussed previously, the IC has policies and processes in place to ensure that data is accurate and, where later determined to be inaccurate or incomplete, is corrected.

VII. **CLPO Findings and Recommendations:**

Based on the foregoing analysis, this assessment finds:

1. Tearline production under ICD 209 relies on information collected and maintained pursuant to both government-wide and IC-specific privacy and civil liberties safeguards, including the Privacy Act (reflecting the FIPPs), FISA, EO 12333 and the IC elements' individual Attorney General Guidelines.

[39] 5 U.S.C. § 552a(e)(7).
[40] See e.g. *Herring v. United States*, 555 U.S. 135 (2009).

2. These privacy and civil liberties safeguards primarily apply to the federal government—more particularly to the IC. Some "downstream" recipients of IC tearlines may not be subject to the similar safeguards or as sensitized to the need to protect identifying information. These concerns can be mitigated by additional measures that:

- Emphasize applicable requirements to alert recipients of inclusion of sensitive or protected information in cyber threat tearlines by use of appropriate control markings (e.g., policies implementing "Controlled Unclassified Information" markings.)

- Request that recipients of tearlines provide feedback about inaccuracy or incompleteness of the PII data received.

- Emphasize analyst training and awareness of civil liberties and privacy issues involved with producing tearlines that include PII.

3. Based on these findings, CLPO recommends that the DNI issue appropriate guidance on analyst training and awareness of privacy and civil liberties issues related to the production of tearlines.

PART X

GENERAL SERVICES ADMINISTRATION

DECEMBER 6, 2013

MEMORANDUM FOR: KAREN L. NEUMAN,
DHS CHIEF PRIVACY OFFICER

MEGAN H. MACK
DHS OFFICER FOR CIVIL RIGHTS AND CIVIL LIBERTIES

FROM: KIM E. MOTT
PRIVACY OFFICER (ISP)

SUBJECT: GSA PRIVACY AND CIVIL LIBERTIES ASSESSMENT, EXECUTIVE ORDER 13636

This memorandum transmits GSA's Privacy and Civil Liberties assessment to the Deparment of Homeland Security, DHS, as required by Executive Order 13636, Improving Critical Infrastructure Cybersecurity. The Privacy and Civil Liberties offices conducted an assessment of activities under this order as stated in Section 5, Privacy and Civil Liberties Protection. Attached is a copy of our assessment.

Thank you.

Attachment

U.S. General Services Administration
1800 F Street NW
Washington, DC 20405
www.gsa.gov

GSA Assessment Report

Executive Order 13636

Improving Critical Infrastructure Cybersecurity

Executive Order

Sec. 5. *Privacy and Civil Liberties Protections.* (a) Agencies shall coordinate their activities under this order with their senior agency officials for privacy and civil liberties and ensure that privacy and civil liberties protections are incorporated into such activities. Such protections shall be based upon the Fair Information Practice Principles and other privacy and civil liberties policies, principles, and frameworks as they apply to each agency's activities.

Executive Order Implementation Activity, GSA:

On February 12th, 2013, the President issued Executive Order 13636[1], Improving Critical Infrastructure Cybersecurity, (EO) directing Federal agencies to use their existing authorities and increase cooperation with the private sector to provide stronger protections for public and private sector cyber-based systems that are critical to our national and economic security. In accordance with the EO, GSA and DoD established a Working Group to fulfill the requirements of Section 8(e) of the Executive Order, specifically:

> *(e) Within 120 days of the date of this order, the Secretary of Defense and the Administrator of General Services, in consultation with the Secretary and the Federal Acquisition Regulatory Council, shall make recommendations to the President, through the Assistant to the President for Homeland Security and Counterterrorism and the Assistant to the President for Economic Affairs, on the feasibility, security benefits, and relative merits of incorporating security standards into acquisition planning and contract administration. The report shall address what steps can be taken to harmonize and make consistent existing procurement requirements related to cybersecurity.*[2]

Assessment Document

In June 2013 the final report of the Department of Defense and General Services Administration was completed. The report "provides strategic guideline for addressing relevant issues, suggesting how challenges might be resolved, and identifying important considerations for the implementation of the recommendations. The ultimate goal of the recommendations is strengthening the cyber resilience of the Federal government by improving management of the people, processes, and technology affected by the Federal Acquisition System. The purpose of the report is to recommend how cybersecurity needs, cyber risk management, and acquisition processes in the Federal government can be better aligned. The report does not provide explicit implementation guidance, but provides

[1] Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 19, 2013).
[2] *Id*.

strategic guidelines for addressing relevant issues, suggesting how challenges might be resolved, and identifying important considerations for the implementation of the recommendations."[3]

The recommendations are as follows:

I. Institute baseline cybersecurity requirements as a condition of contract award for appropriate acquisitions.

II. Address cybersecurity in relevant training.

III. Develop common cybersecurity definitions for federal acquisitions.

IV. Institute a federal acquisition cyber risk management strategy.

V. Include a requirement to purchase from original equipment manufacturers, their authorized resellers, or other trusted sources, in appropriate acquisitions.

VI. Increase government accountability for cyber risk management.

Privacy and Civil Liberties Risks/Impacts:
As this report presents recommendations regarding cybersecurity in the procurement of information and communications technology (ICT), privacy and civil liberties are not directly addressed. However, this document is designed to help agencies address cybersecurity vulnerabilities. By minimizing vulnerabilities, information is more secure, and this includes any privacy material contained in those systems. Each acquired system will need to specifically address proper privacy and civil liberty protections.

FIPPs Analysis:
Transparency:
The report is public so individuals can see what the recommendations are to address cybersecurity regarding acquisition of ICT. The individual systems and related security protocols may not be transparent, but the combined DOD-GSA report is publicly available. The report does not directly impact privacy and civil liberties as personally identifiable information (PII) is not collected, used, or disseminated.

Individual Participation:
There is no individual participation regarding the DOD-GSA report and individual PII is not involved.

Purpose Specification:
The report presents six recommendations regarding cybersecurity with ICT acquisition, and does not impact privacy and civil liberties. No PII is collected or used with this report.

Data Minimization:

[3] Improving Cybersecurity and Resilience through Acquisition. Final Report of the Department of Defense and General Services Administration. June 2013.

The report does not use or generate any data. It just makes recommendations regarding cybersecurity for other agencies to consider when acquiring ICT. Those systems or products will need to address data minimization.

Use Limitation:
There is no use limitation consideration for the activity as it is focused solely on six recommendations regarding ICT acquisition. Those particular acquisitions will need to address use limitation regarding civil liberties and privacy.

Data Quality and Integrity:
There are no data quality and integrity issues for the activity as it is focused solely on six recommendations regarding ICT acquisition. Individual acquisitions will need to address data quality and integrity.

Security:
The report presents six recommendations regarding cybersecurity with ICT acquisition. Those particular acquisitions will address how civil liberties and privacy are impacted, protected, and any necessary compensating controls or measures.

Accountability and Auditing:
No accounting or auditing of the acquisition recommendations is needed as PII is not involved.

Other Privacy and Civil Liberties Considerations:
There are no other privacy and civil liberties considerations for the report and cybersecurity recommendations. The report does mention that privacy is a concern when dealing with critical systems or components, but the report is narrowly tailored to recommendations to address cybersecurity when acquiring ICT. Those individual acquisitions will need to address privacy and civil liberty considerations.

Recommendations:
No recommendations are needed. Agencies should be reminded that, in addition to the cybersecurity recommendations in the report, other considerations, including privacy and civil liberties, should be considered when procuring new ICT.

Appendix

Existing FAR, GSAM, HSAM, and DFARS regulations that include privacy protections.

The FAR (Federal Acquisition Regulation), GSAM (General Services Administration Acquisition Manual), HSAM (Homeland Security Acquisition Manual), and DFARS (Defense Federal Acquisition Regulation Supplement) all have direct references to privacy within their security acquisition language.

FAR, 39.105 Privacy. Agencies shall ensure that contracts for information technology address protection of privacy in accordance with the Privacy Act (5 U.S.C. 552a) and Part 24. In addition, each agency shall ensure that contracts for the design, development, or operation of a system of records using commercial information technology services or information technology support services include the following:
(a) Agency rules of conduct that the contractor and the contractor's employees shall be required to follow.
(b) A list of the anticipated threats and hazards that the contractor must guard against.
(c) A description of the safeguards that the contractor must specifically provide.
(d) Requirements for a program of Government inspection during performance of the contract that will ensure the continued efficacy and efficiency of safeguards and the discovery and countering of new threats and hazards.

FAR, 39.107 Contract Clause. The contracting officer shall insert a clause substantially the same as the clause at 52.239-1, Privacy or Security Safeguards, in solicitations and contracts for information technology which require security of information technology, and/or are for the design, development, or operation of a system of records using commercial information technology services or support services.

Other privacy guidance:

OMB Memo M-12-20 FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management

OMB Memo M-99-05 Instructions on complying with President's Memorandum of May 14, 1998, "Privacy and Personal Information in Federal Records"

OMB Memo M-00-13, Privacy Policies and Data Collection on Federal Web Sites

OMB Memo M-10-23 Guidance for Agency Use of Third-Party Websites and Applications

OMB Memo M-10-22 Guidance for Online Use of Web Measurement and Customization Technologies

OMB Memo of December 29, 2011, Model Privacy Impact Assessment for Agency Use of Third-Party Websites and Applications

OMB Memo M-07-19, FY 2007 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management

OMB Memo M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information

OMB Memo of September 20, 2006, Recommendations for Identity Theft Related Data Breach Notification

NIST Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations

NIST Special Publication 800-144, Guidelines for Security and Privacy in Public Cloud Computing, December 2011.

Executive Order 13402
Strengthening Federal Efforts to Protect Against Identity Theft

Executive Order 13478
Amendments to Executive Order 9397 Relating to Federal Agency Use of Social Security Numbers

Executive Order 13556
Controlled Unclassified Information

Executive Order 13587
Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information

Executive Order 13636
Improving Critical Infrastructure Cybersecurity