

Executive Order 13636 Privacy and Civil Liberties Assessment Report

Compiled by:

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

Department of Homeland Security

July 2016





FOREWORD

July 14, 2016

We are pleased to present the 2016 Executive Orders 13636 and 13691 Privacy and Civil Liberties Assessments Report. On February 12, 2013, President Obama issued Executive Order 13636, *Improving Critical Infrastructure Cybersecurity* and Presidential Policy Directive 21 (PPD-21), *Critical Infrastructure Security and Resilience*, 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. Specifically, Executive Order 13636 requires federal agencies to develop and incentivize participation in a technology-neutral cybersecurity framework, and to increase the volume, timeliness, and quality of the cyber threat information they share with the private sector.

In addition, on February 13, 2015, President Obama issued Executive Order 13691, *Promoting Private Sector Cybersecurity Information Sharing*, which builds upon the foundation established by Executive Order 13636 and PPD-21. Executive Order 13691 specifically acknowledges that organizations engaged in the sharing of information related to cybersecurity risks and incidents play an invaluable role in the collective cybersecurity of the United States. Therefore, the Executive Order encourages the voluntary formation of such information sharing organizations, to establish mechanisms to continually improve the capabilities and functions of these organizations, and to better allow these organizations to partner with the Federal Government on a voluntary basis.

Section 5 of both Executive Orders 13636 and 13691 require that federal agencies coordinate their activities under each Executive Order with their senior agency officials for privacy and civil liberties to ensure that appropriate protections for privacy and civil liberties are incorporated into such activities. Senior agency officials for privacy and civil liberties are also required to annually assess the privacy and civil liberties impacts of the activities their respective departments and agencies have undertaken pursuant to each Executive Order. The senior officials must submit those assessments to the Department of Homeland Security (DHS) Office for Civil Rights and Civil Liberties and the DHS Privacy Office for compilation and publication in this Privacy and Civil Liberties Assessment report.

This third annual report provides assessments of activities under Executive Orders 13636 and 13691 that occurred in fiscal year 2015. With regard to Executive Order 13636, this report builds on last year's report, focusing on programs or activities that are new or have substantially changed within the last fiscal year as a result of the Executive Order's implementation. Since Executive Order 13691 was issued in February 2015, DHS is the only the department or agency

2016 EO 13636 Privacy & Civil Liberties Assessment Report

that performed reportable activities pursuant to the Order in fiscal year 2015. These activities are discussed in DHS’s section of this Privacy and Civil Liberties Assessment report.

The chart below provides an overview of the departments and agencies that provided input for this year’s report pursuant to Executive Order 13636. We note that not all agencies were required to assess all sections of Executive Order 13636. To view the privacy and civil liberties assessments conducted by departments and agencies for previous Executive Order 13636 Privacy and Civil Liberties Assessments Reports, please visit: <https://www.dhs.gov/cybersecurity-and-privacy>.

2016 Executive Order 13636 Section 5 Reports by Department and Topic

| | Department of Homeland Security (DHS) | Department of Treasury (Treasury) | Department of Defense (DoD) | Department of Justice (DOJ) | Department of Health and Human Services (HHS) | Department of Energy (DOE) | Office of the Director of National Intelligence (ODNI) |
|--|---------------------------------------|-----------------------------------|-----------------------------|-----------------------------|---|----------------------------|--|
| 4(a) Cybersecurity Information Sharing | | X | | X | | | X |
| 4(b) Dissemination of Cyber Threat Reports | X | | | X | | | |
| 4(c) Enhanced Cybersecurity Services / Defense Industrial Base Program | X | | X | | | | |
| 4(d) Private Sector Clearance Program | X | X | | | | | |
| 9(a)/9(c) Critical Infrastructure Identification & Notification | | X | | | | | |
| Other | | | | | X | X | |

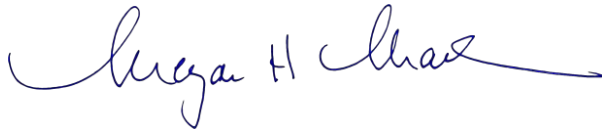
Our offices – the DHS Office for Civil Rights and Civil Liberties and the DHS Privacy Office – coordinated with the senior agency officials for privacy and civil liberties for each reporting agency. This coordination was accomplished with the goal of the reporting senior agency officials assessing and reporting on their respective agencies in an objective and independent manner, consistent with their own authorities and policies. We did not direct the officials in the selection of activities for assessment, their assessment methods, or in the drafting of their reports.

2016 EO 13636 Privacy & Civil Liberties Assessment Report

The reporting senior agency officials did, however, work jointly to produce this report, sharing best practices, following similar formats, and coordinating assessment coverage for sections of Executive Orders 13636 and 13691 being implemented in multiple agencies.

Our offices also facilitated communications among the senior agency officials and the United States Privacy and Civil Liberties Oversight Board (“the Board”) with regard to the privacy and civil liberties assessments conducted under Executive Order 13636. Each agency, however, worked independently and directly with the Board in its consultative role, as specifically required by Section 5 of Executive Order 13636, to maximize the senior officials’ latitude for disclosure and responsiveness to the Board during this process.

Each agency’s report reflects its own senior agency officials’ determination regarding which activities were required under Executive Orders 13636 and 13691, or were otherwise deemed appropriate to be assessed. In future years, as the activities required under each Executive Order are fully implemented across the U.S. Government, senior agency officials will continue to identify, assess, and report on the privacy and civil liberties impacts of new and/or substantially altered programs and activities.

A handwritten signature in blue ink that reads "Megan H. Mack". The signature is fluid and cursive, with a long horizontal stroke extending to the right.

Megan H. Mack
Officer for Civil Rights and Civil Liberties

A handwritten signature in black ink that reads "Karen L. Neuman". The signature is stylized and cursive, with a prominent initial 'K' and a long horizontal stroke extending to the right.

Karen L. Neuman
Chief Privacy Officer

TABLE OF CONTENTS

| | |
|---|-----------|
| FOREWORD..... | 2 |
| PART I: DEPARTMENT OF HOMELAND SECURITY | 6 |
| PART II: DEPARTMENT OF THE TREASURY..... | 23 |
| PART III: DEPARTMENT OF DEFENSE | 46 |
| PART IV: DEPARTMENT OF JUSTICE..... | 50 |
| PART V: DEPARTMENT OF HEALTH AND HUMAN SERVICES..... | 61 |
| PART VI: DEPARTMENT OF ENERGY..... | 66 |
| PART VII: OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE..... | 69 |

PART I: DEPARTMENT OF HOMELAND SECURITY



I. Introduction

Background and Scope

Section 5 of Executive Orders 13636 and 13691 require the DHS Chief Privacy Officer and Officer for Civil Rights and Civil Liberties to assess the privacy and civil liberties impacts of the activities that the Department of Homeland Security (DHS or Department) undertakes pursuant to these Executive Orders and to include those assessments, together with recommendations for mitigating identified privacy risks, in an annual public report. In addition, the DHS Privacy Office and the Office for Civil Rights and Civil Liberties (CRCL) are charged with coordinating and compiling in a single published report the Privacy and Civil Liberties assessments conducted by Privacy and Civil Liberties officials from other Executive Branch departments and agencies with reporting responsibilities under the Executive Orders.

This year's assessment covers Department activities conducted under Executive Orders 13636 and 13691 during fiscal year 2015. Specifically, this year's report provides updates to previous assessments conducted under Executive Order 13636 Sections 4(b), (c), and (d), including explaining instances where implementation approaches have changed. In addition, the DHS Privacy Office and CRCL report the activities that the Department has conducted as a result of Executive Order 13691's issuance in February 2015.

As in the previous 2014 and 2015 Executive Order 13636 assessments, the scope of this year's assessment is limited to those DHS activities that were undertaken as a result of Executive Orders 13636 and 13691 or were substantially altered by these orders. Section 5 of both Executive Orders 13636 and 13691 direct the assessment of "the functions and programs undertaken by DHS as called for in this order," and the scope of the assessment is therefore limited to those functions and programs, rather than attempting to assess the many DHS cybersecurity programs and activities conducted under other authorities. Attempting to include that wide array of programs and activities within this assessment would be impractical, straining oversight office resources, and diluting the in-depth focus on the activities that are driven by Executive Orders 13636 and 13691. More information on DHS's cybersecurity responsibilities and activities is available at: <http://www.dhs.gov/topic/cybersecurity>.

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).¹ 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.

¹ 6 U.S.C. § 142

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 (FIPPs) 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.²

DHS Office for Civil Rights and Civil Liberties

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

- 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.³

² 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>.

³ Detailed information about the activities and responsibilities of the DHS CRCL is available at <http://www.dhs.gov/office-civil-rights-and-civil-liberties>.

DHS Methodology for Conducting Executive Order (EO) 13636/13691 Assessments

Executive Order 13636 and Executive Order 13691 direct senior agency privacy and civil liberties officials of agencies engaged in activities under the orders to perform an “evaluation of activities against the Fair Information Practice Principles (FIPPs) and other applicable privacy and civil liberties policies, principles, and frameworks.” DHS has evaluated its activities against the FIPPs and other applicable privacy and civil liberties policies, principles, and frameworks. More information on the evaluation process is described below.

The DHS Privacy Framework

The FIPPs, which are rooted in the tenets of the Privacy Act of 1974,⁴ 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 Security⁵ and in DHS Directive 047-01, Privacy Policy and Compliance (July 2011).⁶ 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 System of Records Notice (SORN)⁷ and Privacy Impact Assessment (PIA)⁸, as appropriate. There should be no system the existence of which is a secret.

⁴ 5 U.S.C. § 552a

⁵ Available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

⁶ 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.

⁷ The Privacy Act requires that federal agencies issue a SORN to provide the public notice regarding personally identifiable information 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 to demonstrate accountability, and to further the transparency of Department activities. PIAs and SORNs relevant to the Department’s activities under Executive Order Section 4 are discussed in the assessments reported below. The Privacy Point of Contact and Component counsel write the SORN for submission to the Privacy Office. The DHS Chief Privacy Officer reviews, signs, and publishes all DHS SORNs.

⁸ 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.

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.

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 and are the foundation of all DHS privacy-related policies and activities at DHS. DHS uses the FIPPs to assess privacy risks and enhance privacy protections by assessing the nature and purpose of all PII collected to ensure it is necessary for 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. Because the FIPPs serve as the foundation of privacy policy at DHS, the Privacy Office works with Department personnel to complete Privacy Threshold Analyses (PTA)⁹, PIAs, and SORNs to ensure the implementation of the FIPPs at DHS. When conducting a Privacy Compliance Review (PCR)¹⁰, such as the one completed on

⁹ 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.

¹⁰ The DHS Privacy Office exercises its authority under Section 222 of the Homeland Security Act to assure that technologies sustain and do not erode privacy protections through the conduct of PCRs. Consistent with the DHS Privacy Office's unique position as both an advisor and oversight body for the Department's privacy sensitive programs and systems, the PCR is designed as a constructive mechanism to improve a program's ability to comply with assurances made in existing privacy compliance documentation.

the Enhanced Cybersecurity Services (ECS) program,¹¹ the Privacy Office evaluates the program's compliance with the FIPPs, any requirements outlined in its PTA, PIA, or SORN, and any privacy policies that are specific to that program. It is important to note, however, that because DHS uses the FIPPs as its foundational privacy policy framework, many DHS programs or activities do not require specific privacy policies aside from DHS's Privacy Policy Guidance Memorandum on the FIPPs, DHS Directive 047-01 "Privacy Policy and Compliance," and any specific privacy requirements documented in an applicable PTA, PIA, and/or SORN.

Civil Rights and Civil Liberties Assessment Framework

CRCL conducts assessments using an issue-spotting approach rather than a fixed template of issues because the particular issues that may be presented vary greatly across programs and activities. This approach necessitates in-depth factual examination of a program or activity to determine its scope and how it is implemented. Next, CRCL considers the applicability of relevant individual rights protections, first evaluating compliance with those protections, then considering whether a program or activity should modify its policies or procedures to improve the protection of individual rights. As CRCL evaluates programs and activities, consideration is given, but not limited to, the following legal and policy parameters:

- 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 policy concerns are then addressed in policy advice, and sometimes in a formal memorandum or similar document, or in a format comparable to this assessment. CRCL then works with the DHS elements involved, including the Department's Office of the General Counsel, to craft workable policy recommendations and solutions to ensure individual rights are appropriately protected within the assessed program or activity. These solutions may be embedded in program-specific policies, operating procedures, other documentation or simple changes in program activities, as appropriate.

¹¹ See Section III, "EO Section 4(c): Enhanced Cybersecurity Services," for more information on the Privacy Compliance Review.

Related DHS Privacy and Civil Liberties Cyber Activities

Our work under Executive Orders 13636 and 13691 provides further transparency into the Department's cybersecurity-related activities dating back to PIAs and SORNs published in 2004.¹² In addition, the Department has sought the guidance of its Data Privacy and Integrity Advisory Committee (DPIAC)¹³ on cybersecurity-related matters. The DHS Privacy Office has briefed the DPIAC 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, as noted, the DHS Privacy Office and CRCL provide updates to previous assessments conducted under Executive Order 13636 Sections 4(b), (c), and (d). In addition, the DHS Privacy Office and CRCL report the activities that the Department has conducted under Executive Order 13691 since its issuance in February 2015. As the Department continues its implementation activities under these two Executive Orders, the DHS Privacy Office and CRCL will assess new activities, and provide any necessary updates to previous assessments in future reports.

II. EO Section 4(b): Dissemination of Reports

The Secretary and the Attorney General, in coordination with the Director of National Intelligence, shall establish a process that rapidly disseminates the reports produced pursuant to section 4(a) of this order to the targeted entity. Such process shall also, consistent with the need to protect national security information, include the dissemination of classified reports to critical infrastructure entities authorized to receive them. The Secretary and the Attorney General, in coordination with the Director of National Intelligence, shall establish a system for tracking the production, dissemination, and disposition of these reports.

Background

In the 2015 Privacy and Civil Liberties Assessment Report, DHS reported that it participated in a pilot with the Federal Bureau of Investigation (FBI) to determine whether the Cyber Guardian system on the Secret Internet Protocol Router Network (SIPRNET) could be leveraged to track the production and dissemination of cyber threat reports to targeted private sector critical infrastructure entities. As a result of the pilot and with guidance from the National Security Council (NSC) staff, FBI, DHS, and the Department of Defense (DOD) developed an

¹² 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>.

¹³ The DPIAC is a discretionary advisory committee established under the authority of the Secretary of Homeland Security 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>

interagency Joint Requirements Team (JRT) to develop requirements for a system that meets the Section 4(b) mandate.

Since last year's report, the JRT did develop and formalize requirements for a system that meets the Section 4(b) mandate in a Section 4(b) Support Capability Requirements document. On April 10, 2015, the White House Inter-Agency Policy Committee accepted this requirements document and designated the FBI's National Cyber Investigative Joint Task Force (NCIJTF) as the Implementer of the 4(b) Support Capability via the Cyber Guardian System.

Since the White House Inter-Agency Policy Committee accepted the Section 4(b) Support Capability Requirements document in April 2015, the FBI has completed a Memorandum of Understanding (MOU) that participating federal agencies must sign in order to access/use Cyber Guardian and a Rules of Behavior (ROB) document that individual users of the system must sign and with which they must abide. DHS has signed the MOU and all DHS employees currently using the Cyber Guardian system have signed the ROB document as well as completed training on the Cyber Guardian system. Currently, Cyber Guardian enables government agencies with cyber missions to be aware of and de-conflict cyber incidents. Moving forward, Cyber Guardian is the planned platform for cyber incident reports to be assimilated and made available for dissemination to the private sector, and is intended to have the capability to disseminate both unclassified and classified reports to critical infrastructure entities authorized to receive them. Because the NCIJTF maintains and manages the Cyber Guardian system from an engineering and maintenance perspective, additional information on the Cyber Guardian system and its policies may be found in Section 4(b) of this year's Department of Justice (DOJ) Privacy and Civil Liberties Assessment Report.

While the NCIJTF maintains and manages the Cyber Guardian system to track the production and dissemination of cyber threat reports to targeted private sector critical infrastructure entities, DHS continues to develop, receive, and handle cyber threat reports specific to targeted private sector critical infrastructure entities before that information is entered into the Cyber Guardian system. This year's report summarizes DHS's cyber threat reporting under Section 4(b) of Executive Order 13636 and provides a FIPPs assessment conducted by the DHS Privacy Office regarding the cyber threat reporting process.

DHS's Cyber Threat Reporting under Section 4(b)

Typically, DHS law enforcement components discover cyber threat information, specific to a targeted entity, during the course of an investigation. DHS may, however, also encounter cyber threat information in other mission-related activities, such as the protection of federal civilian networks and cyber threat analysis. In addition, targeted private sector entities may voluntarily submit cyber threat information to DHS through the National Cybersecurity and Communications Integration Center (NCCIC) in connection with efforts to protect information systems from known or suspected cybersecurity threats, mitigate such cybersecurity threats, or respond to cyber incidents. DHS shares cyber threat information within the Cyber Guardian system for the purposes of tracking the production, dissemination, and disposition of significant threat reports shared under Section 4 of the Order with U.S. private sector entities so that these entities may better protect and defend themselves against cyber threats and to facilitate proper coordination of victim notifications, in accordance with Section 4(b) of Executive Order 13636 and the Cyber Guardian MOU with FBI.

Privacy Assessment

FIPPs Analysis

Transparency: As noted in the 2014 Report in reference to 4(a) activities, DHS has published a number of PIAs explaining how it currently collects, uses, maintains, and disseminates cyber threat information, including any PII.¹⁴ These PIAs provide generalized notice of DHS's cyber activities as they relate to cyber threats.

The PIA that covers the reporting and collection of cyber threat information from the public and private sector relevant to 4(b) activities is *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 used to defend the federal civilian government's information technology infrastructure from cyber threats. The National Protection and Programs Directorate (NPPD) conducted this PIA because PII may be collected by NCPS, or through submissions of known or suspected cyber threats received by the NCCIC for analysis.

Cyber threat information collected by DHS, specific to targeted private sector critical infrastructure entities, is shared with other Federal agencies that have cybersecurity responsibilities through the FBI's Cyber Guardian system, as detailed in DOJ's Privacy and Civil Liberties Assessment Report of 4(b) activities. Cyber Guardian is employed to track the production, dissemination, and disposition of threat reports shared under Section 4 of the Order with U.S. private sector entities so that these entities may better protect and defend themselves against cyber threats and to facilitate proper coordination of victim notifications.

Data Minimization: Data minimization is at the core of DHS's cyber threat reporting process under Section 4(b) of the Order. As described in the Cyber Guardian MOU with FBI, Cyber Guardian only collects limited PII that is directly relevant and necessary to accomplish the specified purpose of tracking the production, dissemination, and disposition of threat reports shared under Section 4 of the Order and only retains PII for as long as necessary to fulfill this specified purpose. As a result, DHS only enters PII into the Cyber Guardian system that may allow U.S. private sector entities to better protect themselves against cyber threats and to facilitate proper coordination of victim notifications.

Individual Participation: It is not possible to allow individual participation in the context of DHS's sharing cyber threat information with the FBI's Cyber Guardian system and it is not feasible for the Government to provide redress for individuals whose PII may be included in the information submitted to Cyber Guardian.

As stated in the MOU, however, DHS understands that information submitted to Cyber Guardian is subject to applicable federal laws, including but not limited to the Privacy Act, the Freedom of Information Act, the Federal Records Act, and discovery requirements. To the extent information exchanged as a result of Cyber Guardian results in a request or demand for that (or related) information from FBI files pursuant to federal or state civil or criminal discovery or any other request by a third-party for FBI information, such disclosure may only be made after

¹⁴ Available at www.dhs.gov/cybersecurity-and-privacy.

consultation with, and approval by, the FBI and DHS (whose information is at issue), or as otherwise required by law.

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. As it relates to the MOU for DHS's sharing of cyber threat information with the FBI's Cyber Guardian system, the following authorities apply:

1. Privacy Act of 1974, 5 U.S.C. § 552a;
2. Executive Order 13636, Improving Critical Infrastructure Cybersecurity, February 13, 2013;
3. Presidential Policy Directive 21, Critical Infrastructure Security and Resilience, February 12, 2013; and
4. Executive Order 12829, National Industrial Security Program, January 6, 1993, as amended.

Use Limitation: DHS only enters cyber threat reports into the Cyber Guardian system pursuant to Section 4(b) of Executive Order 13636 and the signed Cyber Guardian MOU with FBI. Both state that the information submitted to Cyber Guardian is to be used only for the purposes of tracking the production, dissemination, and disposition of threat reports shared under Section 4 of the Order. In doing so, U.S. private sector entities may better protect and defend themselves against cyber threats and federal agencies may facilitate proper coordination of victim notifications.

Data Quality and Integrity: The cyber threat report information entered into the Cyber Guardian system by DHS, pursuant to Section 4(b) of Executive Order 13636, is derived from existing threat reporting. The data quality and integrity measures in place for those activities are set forth in the NCPS PIA.

Security: DHS accesses the Cyber Guardian application through the secure environment of the SIPRNET, a Department of Defense secret enclave. As explained in the MOU, the use of SIPRNET triggers certain reporting requirements in the event of an unauthorized disclosure. Furthermore, the FBI's ROB for Cyber Guardian sets forth specific rules of behavior, expressly prohibited behavior, and monitoring/search provisions for users of the system.

Accountability and Auditing: As stated in the Cyber Guardian MOU, the FBI monitors, records, and audits use of Cyber Guardian to ensure compliance with applicable laws, regulations, policies, and with the terms of the MOU. If requested by the FBI, each agency that signed the MOU will be responsible for compiling system compliance-related information about its own authorized users and providing that information to the FBI. Such compliance-related information shall include tracking logons and logoffs, creating audit logs, and other appropriate measures, as related to DHS's system.

III. EO Section 4(c): Enhanced Cybersecurity Services

To assist the owners and operators of critical infrastructure in protecting their systems from unauthorized access, exploitation, or harm, the Secretary, 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.

Background

DHS's Enhanced Cybersecurity Services (ECS) was established as a voluntary information sharing program to assist critical infrastructure owners and operators to improve protection of their systems from unauthorized access, exploitation, or data exfiltration. ECS consists of the operational processes and security oversight required to share sensitive and classified cyber threat information with qualified commercial service providers¹⁵ and operational implementers¹⁶ (hereinafter "commercial service providers") that will enable them to better protect their customers, which consist of U.S.-based public and private entities.

DHS reported on the ECS Program in both the 2014 and 2015 Privacy and Civil Liberties Assessment Reports. In the 2014 Privacy and Civil Liberties Assessment Report, DHS focused on discussing key foundational questions in the establishment and operation of the program and the Privacy Office conducted a FIPPs assessment of ECS. In the 2015 Report, DHS provided an overview of the privacy, civil rights, and civil liberties oversight of the program, the assessments of CRCL and the Privacy Office, and a summary of the PCR that the DHS Privacy Office conducted in coordination with the ECS Program and the NPPD Office of Privacy. This year's report provides a brief update on the ECS program's commercial service providers and also addresses the four recommendations from the April 15, 2015, DHS PCR of the ECS Program as discussed in last year's privacy assessment.

ECS Program Update

As explained in the 2015 Privacy and Civil Liberties Assessment Report, NPPD Office of Cybersecurity and Communications (CS&C) provides government furnished information (GFI), specifically indicators of malicious cyber activity,¹⁷ to qualified commercial service providers.

¹⁵ The term Commercial Service Provider (CSP), refers to a public or private company that is capable of providing managed security services for the protection of their customers, which consist of U.S.-based public and private entities. Any managed security service provider meeting the eligibility security requirements may become a CSP.

¹⁶ The term Operational Implementer refers to a critical infrastructure organization that may choose to build its own infrastructure for the purposes of receiving, managing, and utilizing the DHS cyber threat indicators in the protection of its information assets, in effect to act as its own commercial service provider. The requirements for operational implementers are the same as those for commercial service providers. For simplicity, references in this assessment to commercial service providers also apply to operational implementers.

¹⁷ Cyber threats can be defined as any identified efforts directed toward accessing, exfiltrating, manipulating, or impairing the integrity, confidentiality, security, or availability of data, an application, or a federal system, or information processed, controlled, stored on, or transmitting to/from an information system, without lawful authority. Information about cyber threats may be received from government, public, or private sources. Categories

Participating commercial service providers must enter into a memorandum of agreement with DHS and become accredited by achieving a high standard of security competence, including retaining the ability to safeguard sensitive information, obtaining personnel and facilities clearances, and constructing secure network systems as set forth by the security requirements of the ECS Program.

As of the 2014 Assessment cycle, and as noted in the 2015 Privacy and Civil Liberties Assessment Report, only accredited commercial service providers are permitted to provide cybersecurity services to U.S.-based public and private entities. At the time that report was published, only AT&T and CenturyLink were accredited as commercial service providers for ECS. Since the 2015 report was published, however, Verizon and Lockheed Martin have also met the standards for accreditation and are now recognized as ECS Commercial Service Providers. During Fiscal Year 2015, the ECS Program also permitted commercial service providers to extend their ECS customer base beyond those determined to be within the sixteen critical infrastructure sectors, and ECS is now open to all U.S.-based public and private entities.

Update on ECS Privacy Compliance Review Recommendations

As described in the 2015 Privacy and Civil Liberties Assessment Report, the DHS Privacy Office completed a PCR of the ECS Program¹⁸ in coordination with the ECS Program and the NPPD Office of Privacy. The PCR found that NPPD has demonstrated exemplary attention to implementing strong privacy protections in ECS and its related processes, and the DHS Privacy Office provided four recommendations for NPPD in order to further strengthen its privacy protections in ECS and its related processes. These recommendations as well as updates on how they have been addressed by NPPD are described below.

- **Recommendation 1:** NPPD should update the ECS PIA to better reflect the current state of indicator testing and the existing data quality protections DHS is using in the ECS Program.

Update: NPPD has published an ECS PIA Update to reflect the current state of indicator testing. The original PIA stated that ECS indicators were tested for false positives and false negatives in a test environment before sharing with the commercial service providers. The ECS PIA Update clarifies that while testing is a part of the signature development lifecycle as it relates to DHS's deployment of signatures to the .gov domain; ECS shares *indicators* (GFI) with a CSP, not *signatures*. Indicators serve as the basis for an entity to develop a signature within its own unique environment. The CSP may choose to use GFI to develop signatures and would follow its own processes for testing. Consequently, because DHS is sharing indicators for ECS, not signatures, indicator testing is not performed. DHS has other measures to promote data quality including initial and periodic review of indicators which are governed by the program's GFI Data Verification and Vetting Process to ensure GFI is timely, actionable, and vetted by DHS.

of cyber threats may include, for example: phishing, IP spoofing, botnets, denials of service, distributed denials of service, man-in-the-middle attacks, or the insertion of other types of malware.

¹⁸ See "Privacy Compliance Review of the Enhanced Cybersecurity Services (ECS) Program," available at www.dhs.gov/privacy

This process incorporates standard operating procedures that seek to minimize the use or collection of unnecessary PII.

- **Recommendation 2:** NPPD should update the ECS PIA to reflect the current frequency of log reviews.

Update: NPPD has published an ECS PIA Update to clarify that user activity in the National Cybersecurity Protection System, which maintains ECS-related data and information, is logged and the logs are reviewed regularly.

- **Recommendation 3:** NPPD should provide updated information about indicator retention in a future ECS PIA update.

Update: NPPD published the ECS PIA Update to explain that a records retention schedule for NCPS (Records Schedule # DAA-0563-2013-0008) was approved by NARA on January 12, 2015. The NCPS Records Retention Schedule is broken down by five broad capability areas and covers all fields and data collected by and maintained on NCPS, including the voluntary metric information for ECS. The NCPS retention schedule covers all cyber threat information and is not broken down by program. Generally, NPPD will destroy or delete cyber threat information when it is three years old or when it is no longer needed for agency business, whichever is later. Information that is inadvertently collected or determined not to be related to known or suspected cyber threats or vulnerabilities will be destroyed or deleted immediately or when it is no longer needed for agency business (e.g., after the completion of analysis).

- **Recommendation 4:** NPPD should describe in a future ECS PIA update how its subsequent analysis of cybersecurity metrics may lead to the development of new indicators.

Update: The updated ECS PIA explains that NPPD/CS&C provides cybersecurity indicators to commercial service providers, who participate in ECS information sharing, which in turn permits the providers to offer enhanced cybersecurity services to protect the networks of U.S.-based public and private sector entities that request them. The commercial service providers, at the request of ECS participants, use cyber indicators to block known or suspected cyber threats. As part of the program, commercial service providers may share summary information with NPPD/CS&C about the fact that known or suspected cyber threats were detected. This “fact of” occurrence reporting does not contain PII or information that could be considered PII¹⁹. As per the PCR recommendation, NPPD/CS&C is exploring subsequent analysis of data that may lead to the development of new indicators.

¹⁹ DHS uses the phrase “information that could be considered PII” because 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 other information that might be included in the message or subject line. In the context of NCPS, these types of information are not used to identify an individual; instead, they are used as a reference point for particular known or suspected cyber threats.

The DHS Privacy Office has determined the ECS updates explained above and memorialized in the DHS/NPPD PIA Update, DHS/NPPD/PIA-028(a), published on November 30, 2015 are responsive to the PCR recommendations and are considered closed-implemented. Furthermore, these updates do not affect the FIPPs assessment conducted for ECS in the 2014 Privacy and Civil Liberties Assessment Report. Should additional changes take place in the ECS 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 a future Executive Order 13636 Privacy and Civil Liberties Assessment Report.

IV. **EO Section 4(d): Private Sector Clearance Program for Critical Infrastructure**

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.

As discussed in the 2014 Privacy and Civil Liberties Assessment Report, DHS built upon NPPD's Critical Infrastructure Private Sector Clearance Program (since renamed to the Private Sector Clearance Program for Critical Infrastructure (PSCP)) to implement Section 4(d) of Executive Order 13636. Since that time, the PSCP has implemented minor enhancements to better meet the intent of Executive Order 13636 as described below.

Clearance Prioritization Categories: In order to effectively meet the requirements outlined in Section 4(d) of the EO, as well as other critical needs for clearances, the Department developed three categories to prioritize private sector clearance applicants employed by the critical infrastructure owners and operators identified through Section 9 of the Executive Order. DHS assigns the applicant's priority category during the initial application phase. The applicant's priority category remains throughout the clearance package until DHS makes a clearance determination for the applicant. The three categories of prioritization are:

1. Normal Prioritization: This is the default categorization for clearance applications;
2. Time-Critical Prioritization: This is an accelerated process in which the application sponsor has certified a near-term threat requiring a security clearance and a pending classified threat briefing to share that information; and,
3. Expedited Prioritization: This is the fastest option and applies to applications for personnel of critical infrastructure owners and operators, in which "a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security," as identified in Section 9 of EO 13636.

Applications designated as Time-Critical or Expedited receive priority processing at each phase of the application process.

Updated DHS Form 9014: With the enhancements to the PSCP, NPPD's Office of Infrastructure Protection expanded the DHS Form 9014, *Critical Infrastructure Private Sector Clearance Program Request*, to collect additional information from qualified PSCP Nominees

2016 EO 13636 Privacy & Civil Liberties Assessment Report

who require clearances based on their day-to-day work related to the security and protection of critical infrastructure. As it relates to Executive Order 13636, these PSCP Nominees include, in part, the private sector clearance applicants employed by the critical infrastructure owners and operators identified through Section 9 of this Executive Order. As a result, PSCP Nominees must now provide the following information via the updated DHS Form 9014 (*Note: (*) denotes a new data element requested on the updated DHS Form 9014*):

- Full name;
- Company name and address;
- Business phone number;
- Business email address;
- Level of clearance requested;
- Current association memberships;
- U.S. Citizen (yes/no);
- Justification to access classified information (to include Nominee's job title, position, and responsibilities);
- Information regarding whether the Nominee's company Chief Security Officer (or the executive otherwise responsible for the Nominee organization's security posture) has been notified of the Nominee's nomination (yes/no/N/A);*
- Information regarding whether there is a secure facility within 50 miles where a clearance holder may attend a classified briefing (yes/no/no, but willing to travel);*
- Information pertaining to how the Nominee satisfies the criteria for PSCP nomination (checkboxes provide the criteria selection from EO 135497);* and,
- Nominee's sector.

If the Nominee has held an active clearance within the past 24 months, then the Nominee must also provide:

- Whether he or she previously held or currently holds a clearance and what type of clearance he or she held or holds (Secret/Top Secret);
- The name of the Agency that sponsored the clearance;
- Contact information for his or her Security Official/Office (phone number and email address);
- Information regarding whether he or she is retired or separated or if he or she is planning on retiring and separating from the position in which he or she held an active clearance within the past 24 months (to include from where the Nominee is retiring or separating);
- If the Nominee is retired or separated, then he or she must also provide his or her date of retirement or separation;
- Reciprocity/reinstatement (yes/no (Nominees may only select "yes" if they have a current clearance or if their prior security clearance was active within the last 2 years));* and,
- If a PSCP clearance holder is undergoing a reinvestigation, then he or she must provide information regarding how recently he or she used the PSCP clearance (No, Yes-within the past year, Yes-within the past 2 years, Yes-within the last 5 years, or Yes-within the last 10 years).*

These new data elements were added to improve the program's overall effectiveness. For example, the PSCP is now requesting that Nominees provide information regarding whether or not they are located within 50 miles of a secure facility for classified briefings. This information will help the program determine the best way to deliver classified information to the PSCP Nominee if and when he or she is provided with a clearance. Furthermore, the updated DHS Form 9014 requests information from PSCP clearance holders undergoing reinvestigations regarding how often they have used their federal security clearance. This information will provide the PSCP with a better understanding of whether a clearance holder should continue to hold a federal security clearance in order to perform his or her duties.

The DHS Privacy Office determined that the changes do not alter the FIPPs assessment conducted for the PSCP in the 2014 Privacy and Civil Liberties Assessment Report. These changes were, however, captured in a DHS/NPPD Privacy Impact Assessment Update, DHS/NPPD/PIA-020(a) - Private Sector Clearance Program for Critical Infrastructure, which was published on February 11, 2015. 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 a future Executive Order 13636 Privacy and Civil Liberties Assessment Report.

V. *Executive Order 13691, Promoting Private Sector Cybersecurity Information Sharing*

Background

On February 13, 2015, President Obama signed Executive Order 13691, *Promoting Private Sector Cybersecurity Information Sharing*, to build upon the foundation established by Executive Order 13636 by encouraging the development of information sharing and analysis organizations (ISAO) to serve as focal points for cybersecurity information sharing and collaboration within the private sector and between the private sector and Government. Specifically, Executive Order 13691:

- Directs the Secretary of DHS to strongly encourage the development and formation of ISAOs;
- Directs DHS to select, through an open and competitive process, a non-governmental organization to serve as the ISAO Standards Organization. This ISAO Standards Organization will identify a set of voluntary standards or guidelines for the creation and functioning of ISAOs;
- Streamlines the mechanism for DHS's NCCIC to enter into information sharing agreements with ISAOs. This will ensure that robust, voluntary information sharing continues and expands between the public and private sectors;
- Directs DHS to develop a more efficient means for granting clearances to private sector individuals who are members of an ISAO via a designated critical infrastructure protection program; and,
- Adds DHS to the list of federal agencies that approve classified information sharing arrangements.

The purpose of the ISAOs is to permit sharing of cyber threat information among a broader group of sharing and analysis organizations than is presently feasible. Current cyber threat information sharing among groups of this type is focused on Information Sharing and Analysis

Centers, which are linked to the 16 Critical Infrastructure Sectors and the corresponding Sector-Coordinating Councils. The effort to suggest model information sharing structures to ISAOs responds to the independent establishment of voluntary participation cyber threat analysis and sharing organizations that are not tied to Critical Infrastructure Sectors. Expanding the scope of this information sharing – with appropriate privacy and civil liberties safeguards – will enable the Department to provide robust support to diverse groups that may be organized around regional cybersecurity interests, non-critical infrastructure industry or commerce interests, or other communities of interest seeking to voluntarily and collectively improve their cybersecurity posture.

Executive Order 13691 Update

Following the competitive process directed by Section 3(a) of the Order, the Department selected, as the ISAO Standards Organization, the University of Texas at San Antonio (UTSA) with support from Logistics Management Institute (LMI) and the Retail Cyber Intelligence Sharing Center (R-CISC). This ISAO Standards Organization will result in the promulgation of model practices standards for ISAOs, and, it is hoped, lead to the widespread establishment of ISAOs. ISAOs will serve as focal points for cybersecurity information sharing and collaboration within the private sector and between the private sector and government. Per Executive Order 13691, the UTSA team will work with existing information sharing organizations, owners and operators of critical infrastructure, relevant agencies, and other public and private sector stakeholders to identify a common set of voluntary standards or guidelines for the creation and functioning of ISAOs.

DHS has participated in other activities in implementing Section 2(a) of the Executive Order. DHS led three public workshops with the private sector to receive feedback on some of the requirements that the selected ISAO Standards Organization should focus on upon selection. These workshops were held on the following dates and locations:

- April 20, 2015 in San Francisco, CA (partnered with White House and PricewaterhouseCoopers);
- June 9, 2015 in Cambridge, MA; and,
- July 30, 2015 in San Jose, CA.

DHS also provided over 25 briefings to private sector and Government organizations during that time frame to provide transparency into the process, discuss the development and formation of ISAOs, and encourage participation.

Although the Department has undertaken significant activities to implement Executive Order 13691, our offices determined that none of the activities directed by the Order are in a posture that is suitable for privacy or civil liberties assessment at this time. The DHS Privacy Office and CRCL will continue to monitor the progress of the Department's Executive Order 13691 activities and will assess these activities, as appropriate, in future Privacy and Civil Liberties Assessment Reports.

PART II: DEPARTMENT OF THE TREASURY



DEPARTMENT OF THE TREASURY ASSESSMENT OF THE IMPLEMENTATION OF E.O. 13636, “IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY”

Introduction

On February 12, 2013, the President signed Executive Order (“EO” 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.”

To ensure the inclusion of privacy and civil liberties protections in activities under the Order, Section 5(a) requires federal agencies to coordinate EO-related cybersecurity activities with their senior agency officials for privacy (“SAOP”). Section 5(b) further requires the SAOP to conduct an assessment of their agency’s activities under the Order and to submit to the Department of Homeland Security (“DHS”) its assessment for consideration and inclusion in a public report that shall be reviewed on an annual basis.

The Department of the Treasury (“Treasury” or “Department”) is engaged in activities under the EO, and the Department’s SAOP submits the following assessment of Treasury’s activities conducted during the October 1, 2014 to September 30, 2015 reporting period.

Treasury’s Privacy and Civil Liberties (PCL) Organization and Processes

Within Treasury, the Assistant Secretary for Management (“ASM”) is responsible for the overall implementation of privacy and civil liberties requirements. Treasury Order 102-25, “Delegation of Authority Concerning Privacy and Civil Liberties,” designates the ASM as the Department’s SAOP, Chief Privacy and Civil Liberties Officer, and Information Sharing Environment Privacy Official.

At Treasury, the Deputy Assistant Secretary for Privacy, Transparency, and Records (“DASPTR”) is the ASM’s principal advisor on privacy and civil liberties matters. The DASPTR is responsible for establishing Treasury-wide policies, procedures, and standards to ensure the Department’s full compliance with federal laws, regulations, and policies relating to information privacy.

Overview of 13636 Relevant Activities

Fostering the stability of financial markets and institutions is an integral component of Treasury’s leadership, domestically and globally. A secure and resilient financial system is at the heart of our Nation’s economic prosperity and Treasury’s primary objective since 1789.

In 1998, the President issued Presidential Decision Directive (“PDD”) 63, identifying telecommunications, banking and finance, energy, transportation, and essential government services as vulnerable sectors. In the PDD, the President appointed Treasury as the lead agency for liaison with the banking and finance sector as part of a national effort to assure the security of the United States’ increasingly vulnerable and interconnected infrastructures. In 1999, as part of this effort, Treasury supported the creation and development of the Financial Services Information Sharing and Analysis Center, which is one of the oldest private information-sharing Initiatives in the United States.

Following the attacks of September 11, 2001, Treasury established the Office of Critical Infrastructure Protection and Compliance Policy (“OCIP”), chaired a newly formed Finance and Banking Information Infrastructure Committee comprised of financial regulators, and encouraged the establishment of the Financial Services Sector Coordinating Council of private sector institutions and organizations.

Homeland Security Presidential Directive 7 (“HSPD 7”), released in 2003, superseded PDD 63 and reaffirmed Treasury’s role as sector liaison by naming Treasury the Sector Specific Agency (“SSA”) for finance and banking, while recognizing the importance of the roles played by the Departments of Homeland Security, State, Justice, Commerce, and Defense in protecting our nation’s national infrastructure protection across all sectors.

Presidential Policy Directive (“PPD”) 21, which superseded HSPD 7 in 2012, continued to advance a unified approach to strengthening and maintaining secure, functioning, and resilient critical infrastructure against both cyber and physical threats. PPD 21 identifies 16 critical sectors, reaffirming Treasury as SSA for the Financial Services Sector.

In its capacity as the SSA for the Financial Services Sector, Treasury is the day-to-day federal interface and coordinating agency for various interagency and public-private partnership activities relating to the security and resilience of the Financial Services Sector’s critical infrastructure. These responsibilities generally are carried out through OCIP, which is part of the Treasury Office of Financial Institutions. OCIP facilitates implementation of EO 13636 as described below.

Treasury’s Continued Activities under the EO for the Reporting Period

Treasury’s activities under the EO have not materially changed since we last reported. Treasury continues to play a minor role in two programs that distribute personally identifiable information (PII): Information Sharing under section 4(a) of the EO, and the Critical Infrastructure Private Sector Clearance Program under section 4(d) of the EO. In addition, Treasury continues to play a minor role in identifying critical infrastructure where a cybersecurity incident could reasonably result in catastrophic consequences (“high risk critical infrastructure”), as required under section 9(a) of the EO.

As the SSA for the Financial Services Sector, Treasury continues to receive requests for nominations for national security clearances to allow financial services critical infrastructure owners, operators, and sector leaders to access cyber threat information. Through a consultative

process required by EO 13636, Treasury continues to assist law enforcement and national security agencies with identifying high risk critical infrastructure.

During the FY 2015 reporting period, the Cyber Intelligence Group (CIG)²⁰ of Treasury's Office of Critical Infrastructure Protection and Compliance Policy (OCIP) held monthly classified cyber information meetings for cleared financial sector representatives, and, separately, for cleared financial regulators to increase the volume, timeliness, and quality of cyber threat information shared with the U.S. financial sector under Section 4 of EO 13636. This activity is consistent with our responsibilities under the EO that we assessed in previous reports.

Summary of Assessment Methodology

The Fair Information Practice Principles ("FIPPs") are a set of internationally recognized principles designed to ensure the protection of information privacy protections. Treasury uses the FIPPs as the general framework to analyze Treasury's collection, use, maintenance, and sharing of PII.

Detailed Analyses of Private Sector Clearance Program under 4(d) of EO 13636

Section 4(d): Private Sector Clearance Program

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. . . .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.

Detailed Description of Private Sector Clearance Program

As the SSA for the Financial Services Sector, Treasury receives requests for access to cyber threat information from financial services critical infrastructure owners, operators, and sector leaders (i.e., Sector Coordinating Council members). Treasury recognizes that cyber threat information may include classified information and that an individual must have an active national security clearance prior to receiving classified information from the government. Therefore, to allow owners, operators, and sector leadership to receive classified cyber threat information, Treasury nominates appropriate individuals for national security clearances.

In this program, Treasury receives requests for security clearances from DHS and the private sector. DHS is responsible for providing forms to Treasury for distribution and for referring

²⁰ The CIG consists of a specialized team of analysts with expertise in financial services, cybersecurity, and intelligence analysis. The CIG's primary function is to distribute timely and actionable information and analysis that financial institutions can use to protect themselves from cyber attacks.

individuals in the Financial Services Sector to Treasury for formal nomination. Private sector clearance candidates are required to complete certain sections of DHS Form 9014. Individuals from the Financial Services Sector submit a partially completed DHS Form 9014 to Treasury. A Treasury employee verifies that the private sector clearance candidate has completed the necessary sections of the form. The Treasury employee signs the form, nominating the individual for a security clearance, and sends the form to DHS as an attachment via encrypted electronic mail and deletes the form from Treasury systems. Once DHS receives the form, a DHS employee works directly with the nominee in the clearance process.

Description of Assessment Methodology

To facilitate the processing of national security clearances for appropriate Financial Services Sector personnel, Treasury participates in the DHS Critical Infrastructure Private Sector Clearance Program (“DHS Private Sector Clearance Program”). This program is a government-wide service that provides a means for expediting the processing of national security clearance applications for private sector partners. Treasury is responsible for initiating the nomination process for Financial Services Sector security clearance nominees. Once nominated, DHS and the Office of Personnel Management (“OPM”) are responsible for conducting the investigation necessary to adjudicate national security clearances for nominated private sector individuals. The data collected for security clearances is not used for any purpose other than assisting with securing a clearance. A full assessment of the DHS Private Sector Clearance Program is included in the DHS portion of the 2015 Executive Order 13636 Privacy and Civil Liberties Assessments Report.

Treasury uses the FIPPs to assess cybersecurity programs for potential privacy issues. The FIPPs are:

1. Transparency: Treasury should be transparent and provide notice to the public regarding its collection, use, sharing, and maintenance of PII.
2. Individual Participation: Treasury should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the collection, use, sharing, and maintenance of PII. Treasury should also provide mechanisms for appropriate access, correction, and redress regarding Treasury’s use of PII.
3. Purpose Specification: Treasury should specifically articulate the authority that permits the collection of PII and the purpose or purposes for which the PII is intended to be used.
4. Data Minimization: Treasury 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).
5. Use Limitation: Treasury should use PII solely for the purpose(s) specified in required information notices (e.g., systems of records notices). Sharing of PII outside the Department should be done in a manner compatible with the purpose for which the PII was originally collected.
6. Data Quality and Integrity: Treasury should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete.

7. Security: Treasury 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.
8. Accountability and Auditing: Treasury 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.

Civil liberties are those basic rights and freedoms guaranteed to individuals. As recognized by the EO and its associated guidance, these Constitutional rights may be implicated by cybersecurity programs that monitor lawful activities or communications. Therefore, in addition to its FIPPs analysis, Treasury will consider whether agency EO activities involve the monitoring or interception of communications, or compiling of information regarding lawful activities that may impact civil liberties. Treasury will also consider the legal authorities that support such activities and the procedures undertaken to safeguard individual rights in carrying out such activities.

Privacy and Civil Liberties (PCL) Assessment of Private Sector Clearance Program

PCL Protections and Compliance

All PII collected within this activity is stored on a Treasury system. Permission to access this information is granted on a need to know basis to protect the information collected. Information is stored within the Treasury network on a temporary basis only. Treasury acts as a facilitator in this process, so the PII submitted for clearance purposes is not shared with or used by any other Treasury programs. The majority of this activity is performed by DHS. Therefore, that Department handles the majority of the PCL protections and compliance associated with it.

| Protections | Response |
|--|--|
| Are individuals provided notice at the time of collection regarding why the information is being collected and how it will be used? | Treasury uses DHS Form 9014, “Critical Infrastructure Private Sector Clearance Program Request,” to collect the limited set of PII necessary to nominate an individual for a national security clearance. A Privacy Act statement is provided to individuals at the time they receive the form advising them of why the information is being collected and how it will be used. |
| Please describe how the program removes data that is no longer necessary | Individuals identified by their organization or by DHS electronically mail Treasury a partially completed DHS Form 9014. Once received, Treasury reviews the information and nominates the individual by forwarding the form to DHS. While in Treasury’s custody, the DHS Form 9014 is a working paper. Once DHS receives it, DHS is responsible for maintaining and disposing the form under General Records Schedule 18, Number 22, <i>Personnel Security Clearance Files</i> . Once DHS confirms the receipt of |

| Protections | Response |
|---|--|
| | <p>DHS Form 9014, any copies of such form maintained at Treasury are working papers. As working papers in a DHS system of records, Treasury is no longer responsible for maintaining them. Once Treasury receives confirmation from DHS that it received the form, Treasury deletes the partially completed DHS Form 9014 from its system.</p> |
| <p>Please describe any steps taken to mitigate any use of PII that is not specified in the applicable notices.</p> | <p>Once received, Treasury reviews all DHS Form 9014s. Treasury employees complete two steps: first, they review information only to ensure that the proper boxes have been filled in and then they formally nominate the individual by electronically mailing the DHS Form 9014 to DHS. While Treasury reviews the form for completeness, it is stored in a local folder, with access limited to only those who have a need to know the information to perform their duties.</p> |
| <p>Please describe any safeguards that are in place to ensure the continued security of data maintained within the system.</p> | <p>Information Treasury collects in support of the DHS Private Sector Clearance Program is sent directly from the private sector clearance candidate to Treasury by electronic mail. AES 256 bit Encryption is deployed by the Treasury Network for encrypting external traffic from the Departmental Offices Local Area Network (“DO LAN”). DO LAN employs technology that scans for viruses, malware, spam, and other dangerous or suspicious signatures before being delivered to mailboxes. Anything identified as potentially harmful to PII being sent to Treasury employees is quarantined in a secure container until it can be handled properly. While Treasury reviews the DHS Form 9014 for completeness, it is stored in a Treasury local shared drive folder with restricted access. Treasury’s non-classified electronic mail and local shared drives are maintained on the DO LAN. The DO LAN is rated as a Federal Information Security Management Act HIGH system, meaning that the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. The safeguards applied to the DO LAN reflect the sensitivity of the information it contains.</p> |
| <p>Please describe the method for securing data at rest in the system.</p> | <p>Treasury employs Microsoft Active Directory’s role based access controls to prevent unauthorized access to data at rest on the DO LAN. This directory helps ensure that employees and contractors who do not have a need to access the information stored in this program do not have privileges to access the information.</p> |
| <p>What methods are in place to audit access to records</p> | <p>Treasury deploys a Splunk Enterprise solution to allow for auditing of user activities on the DO LAN. The solution monitors role based access controls assigned to the files and</p> |

| Protections | Response |
|--|--|
| maintained within the system? | folders in which Treasury temporarily stores DHS Form 9014s. This helps Treasury prevent employees who have access to the information to perform their official Treasury functions from exceeding their authority by accessing and/or using the information for unauthorized purposes. |
| Please describe any agency oversight mechanisms that apply to the system. | <p>Private sector clearance candidates send their information in support of the DHS Clearance Program to Treasury by electronic mail. While Treasury reviews the DHS Form 9014 for completeness, it is stored in a local shared drive folder. Treasury’s non-classified electronic mail and shared drives are maintained on the DO LAN, a system secured at the highest level for a non-classified system. There is no way to guarantee that electronic mail sent to Treasury from outside entities is encrypted.</p> <p>All Treasury information systems used to process and store PII undergo a mandatory security assessment and authorization (“SA&A”) process to verify that the system provides adequate measures to preserve the confidentiality, integrity, and availability of all sensitive information residing on or transiting those systems. A Privacy Impact Assessment (“PIA”) is required as part of the SA&A process. The PIA for the DO LAN was completed on Dec 4, 2007. A revised and updated Privacy and Civil Liberties Impact Assessment (“PCLIA”) for the DO LAN is currently in development.</p> |

PIAs or Other Documentation

DHS Form 9014s are stored only on the DO LAN while they are reviewed for completeness. The PIA for the DO LAN was completed on Dec 4, 2007 and is currently being updated. A PIA is not required when information contained in a system relates to internal government operations or when it has been previously assessed under an evaluation similar to a PIA.

FIPPS and/or Civil Liberties Analysis:

| Transparency: | Response: |
|---|--|
| How is the general public informed about the DHS Critical Infrastructure Private Sector Clearance Program? | DHS is the lead agency for the DHS Private Sector Clearance Program. Pursuant to the E-Government Act of 2002 and Office of Management and Budget (OMB) Memorandum 03-22, “OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002,” DHS last published a PIA for the program on February 11, |

| | |
|--|---|
| | 2015. . The PIA, which informs the general public about this program, is available to the general public on the DHS Privacy Office’s website. ²¹ |
| When collecting information from members of the public, does the program submit documentation for an OMB Collection number? | Yes. The collection number for DHS Form 9014 is OMB No. 1670-0013. DHS last published notice of the form in the <i>Federal Register</i> on September 24, 2014. See <i>Federal Register</i> Docket Number DHS-2014-0007. |
| Does the agency operate a Privacy Act system of records in support of the DHS Critical Infrastructure Sector Clearance Program? | Treasury does not operate a Privacy Act system of records in support of the DHS Sector Clearance Program. Once Treasury transmits the DHS Form 9014 to DHS, the system of records notice entitled DHS/ALL–023 Department of Homeland Security Personnel Security Management, 75 FR 8088 (February 23, 2010) covers the information. |
| How does this program ensure that notices are updated to reflect system or program changes? | As the lead agency for the DHS Private Sector Clearance Program, DHS is responsible for ensuring that its PIA is updated to reflect system or program changes. This report also serves to provide notice to the public about the privacy safeguards deployed in the implementation of the DHS Private Sector Clearance Program. Treasury does not maintain any additional notices with respect to its supporting role in the DHS Private Sector Clearance Program. A PIA is not required when information contained in a system relates to internal government operations; when it has been previously assessed under an evaluation similar to a PIA. |

| Individual Participation: | Response: |
|--|--|
| Are individuals asked for consent and given the opportunity to object to the collection of their PII? | Yes. Individuals in the Financial Services Sector who have been identified by their organization or by DHS as needing access to classified cyber threat information may complete DHS Form 9014 and securely transmit it by electronic mail to Treasury to start the nomination process. There is a Privacy Act Statement in the form providing notice to individuals regarding DHS’s use of the information. Participation in the DHS Private Sector Clearance Program is voluntary. Individuals who do not approve of DHS’s use of the information as stated in DHS Form 9014 have the opportunity to object to collection of their PII by not completing and submitting the form for review. By completing and submitting the form, the individuals consent to the collection of the contents of the form. The individual is not required to submit information for a clearance, but |

²¹ The DHS PIA for the Private Sector Clearance Program is available here: <https://www.dhs.gov/sites/default/files/publications/privacy-pia-nppd-pscp-february2015.pdf>

| | |
|--|--|
| | refusal to submit the information will result in their inability to secure a clearance. |
| Are individuals given the opportunity to access and correct their PII? | Yes, nominees have the opportunity to access and correct information submitted using the DHS Form 9014. Access and correction procedures are described in the DHS Critical Infrastructure Private Sector Clearance Program PIA, which is available to the public through the DHS Privacy Office website. A PIA is not required when information contained in a system relates to internal government operations; when it has been previously assessed under an evaluation similar to a PIA. |
| Describe the mechanism provided for an individual to seek redress in the event of inappropriate access to or disclosure of their PII. | If inappropriate access or disclosure gave rise to sufficient risk to the individual or Treasury, Treasury would provide notification to the individual as required in Treasury Directive (TD), 25-08, <i>Safeguarding Against and Responding to the Breach of PII</i> . If notification is given under TD 25-08, the notice would provide a point of contact to whom questions may be directed. If questions evolve into a complaint, the complaint will be addressed by the Office of Privacy, Transparency, and Records working in conjunction with the Office of General Counsel and the Office of Public Affairs. |

| Purpose Specification: | Response: |
|--|---|
| Please provide the specific purpose(s) for the maintenance of PII within the system | Treasury collects PII from individuals in the Financial Services Sector who their organization or DHS has identified as needing access to classified cyber threat information. After DHS or sector representatives identify individuals who need a clearance, the private sector clearance candidate completes the form and sends it to Treasury. Treasury disposes of the information after it ensures the DHS Form 9014 is completed according to the form’s directions, securely transmits the completed form to DHS, and receives notice of receipt from DHS. |
| What steps are taken to ensure the authority for the collection is valid? | Pursuant to PDD 21, “Critical Infrastructure Security and Resilience,” Treasury is the SSA for the Financial Services Sector. In this role, and in support of the EO, Treasury may nominate individuals from the sector for national security clearances. Treasury is responsible for verifying that individuals in the process are associated with the Financial Services Sector. |

| Data Minimization: | Response: |
|--|---|
| <p>Please describe the data elements that are relevant and necessary.</p> | <p>To initiate the process, individuals complete the DHS Form 9014 and send the following information to Treasury: name, company name/address, phone number, e-mail address, level of clearance, and citizenship. Treasury then securely transmits this information to DHS after reviewing it for completeness.</p> <p>Employees of the Office of Privacy, Transparency, and Records have conducted several meetings with OCIP to ensure that any PII distributed has been minimized and is only used for its original stated purpose. As the SSA for the Financial Services Sector, it has been determined that Treasury’s knowledge of the Financial Services Sector is instrumental in the decision making process for identifying individuals within the sector who require clearances.</p> |

| Use Limitation: | Response: |
|--|---|
| <p>Please describe the steps taken to ensure the use of PII is limited to the purpose(s) specified in applicable notices.</p> | <p>PII that Treasury receives for the DHS Critical Infrastructure Private Sector Clearance Program is limited to the information submitted by the nominee using DHS Form 9014. Once identified, Treasury directs private sector clearance candidates to submit the DHS Form 9014 to a secure Treasury electronic mail inbox that is dedicated to receipt of these forms. Access to the dedicated inbox is limited to Treasury employees and contractors who have a need to know. Treasury does not share DHS Form 9014s with any other Treasury bureaus or offices and only shares them externally with DHS. Information collected in this program is only used for its original purpose.</p> |

| Data Quality and Integrity: | Response: |
|--|--|
| <p>What steps are taken to ensure the continued quality and integrity of data maintained by the project or system?</p> | <p>Information Treasury collects in support of the DHS Critical Infrastructure Private Sector Program is sent directly from the potential nominee to Treasury by electronic mail. Treasury, in turn, sends the information on to DHS using encrypted electronic mail. DHS then contacts the nominee directly to provide the additional information necessary to complete the remaining DHS Form 9014 fields.</p> |
| <p>What steps are taken to ensure information maintained in the system is accurate, timely, relevant, and complete?</p> | <p>After DHS receives the DHS Form 9014 from Treasury and collects additional information from the private sector nominee/clearance candidate to complete the form, DHS provides to OPM the information necessary to begin the background investigation. OPM then works directly with</p> |

| | |
|---|--|
| | nominees to ensure that the information provided to Treasury and DHS is accurate, timely, and complete. Nominees are provided the opportunity to correct inaccurate or erroneous information. Any inaccurate or outdated information provided to Treasury is thereby corrected by either DHS or OPM. |
| Please describe the method for eliminating PII that is no longer needed. | Information collected by Treasury in support of the DHS Private Sector Clearance Program is sent directly from the potential nominee to Treasury by electronic mail. While the DHS Form 9014 is being reviewed by Treasury, the form is stored in a Treasury local shared drive folder with access limited to personnel and contractors who have a need to know. After Treasury electronically mails the partially completed form to DHS and receives confirmation from DHS that it received the form, Treasury deletes the partially completed DHS Form 9014. |

| | |
|--|---|
| Security: | Response: |
| Please describe any safeguards that are in place to ensure the continued security of data maintained within the system. | Information collected by Treasury in support of the DHS Private Sector Program is sent directly from the potential nominee to Treasury by electronic mail. While the DHS Form 9014 is being reviewed by Treasury, it is stored in a Treasury local shared drive folder with access limited to personnel and contractors who have a need to know. Treasury's non-classified electronic mail and local shared drives are maintained on the DO LAN. The safeguards applied to the DO LAN reflect the sensitivity of the information it contains. |
| Please describe the method for securing data at rest in the system. | Treasury employs Microsoft Active Directory's role based access controls and audit controls to prevent unauthorized access to or use of data at rest on the DO LAN. |
| If data from the system is sent electronically, what methods are in place to ensure appropriate safeguards apply? | Private sector clearance candidates send the partially completed DHS Form 9014 to a secure Treasury electronic mail inbox dedicated to receiving these forms. Treasury then reviews the form for completeness and forwards it via encrypted electronic mail to DHS. AES 256 bit Encryption is deployed by Treasury Network for encrypting external traffic from the DO LAN. |

| | |
|---|--|
| Accountability and Auditing: | Response: |
| What methods are in place to audit access to records | Treasury deploys a Splunk Enterprise solution to audit user activities on the DO LAN. The solution monitors role based |

| | |
|---|--|
| <p>maintained within the system?</p> | <p>access controls assigned to files and folders in which Treasury temporarily stores DHS Form 9014s.</p> |
| <p>Please describe any agency oversight mechanisms that apply to the system.</p> | <p>All Treasury information systems used to process and store PII undergo a mandatory SA&A process to verify that the system provides adequate measures to preserve the confidentiality, integrity, and availability of all sensitive information residing on or transiting those systems. Treasury information security professionals oversee completion of the SA&A process. A PIA is required as part of the SA&A process.</p> <p>Treasury also deploys a Splunk Enterprise solution to audit user activities on the DO LAN. The solution monitors role based access controls assigned to files and folders in which Treasury temporarily stores DHS Form 9014s.</p> <p>The PIA for the DO LAN was completed on Dec 4, 2007. A revised and updated PCLIA for the DO LAN is currently in development. A PIA is not required when information contained in a system relates to internal government operations or when it has been previously assessed under an evaluation similar to a PIA.</p> |

| |
|---|
| <p>Civil Liberties Considerations:</p> |
| <p>The Office of Privacy, Transparency, and Records reviewed this activity, its standards, and the criteria for participation in it. At this time, there is no Privacy and Civil Liberties Impact Assessment for DO LAN that specifically addresses the information in this program. Treasury is currently working on an updated Privacy and Civil Liberties Impact Assessment for the DO LAN that will address the privacy and civil liberties information in this program.</p> |

PCL risks/impacts:

| | |
|---|--|
| <p>Risk:</p> | <p>Impact:</p> |
| <p>Please explain the possibility of redress if data is lost due to an email breach.</p> | <p>If inappropriate access or disclosure gave rise to sufficient risk to the individual or Treasury, Treasury would provide notification to the individual as required in TD 25-08, <i>Safeguarding Against and Responding to the Breach of PII</i>. If notification is given under TD 25-08, a relevant point of contact would be given, to whom questions may be directed.</p> <p>If questions evolve into a complaint, the complaint will be addressed by the Office of Privacy, Transparency, and Records.</p> |

| | |
|--|--|
| Please describe the method for ensuring that access to data maintained within the system is limited to individuals with a need to know. | Identity verification for access to information maintained on the DO LAN includes the use of personal identity verification cards, usernames, and passwords. |
|--|--|

Private Sector Clearance Program Summary

Treasury has conducted its review for the reporting period and has determined that the limited role the Department plays in the Private Sector Clearance Program raises no broader PCL issues, policy considerations, nor legal considerations. Treasury will continue to evaluate its role in the program and may develop a more thorough privacy assessment, as that role expands or changes for future reports.

Detailed Analyses of Cyber Security Information Sharing Under 4(a) of EO 13636

Section 4(a): Cyber Security Information Sharing²²

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 they may better protect and defend themselves against cyber threats.

Detailed Description of Cyber Security Information Sharing

To increase the volume, timeliness, and quality of cyber threat information shared with U.S. financial sector entities so they may better protect and defend themselves against cyber threats, Treasury requests declassification of and subsequently disseminates relevant law enforcement and intelligence information to the financial sector (including financial regulators) and other critical infrastructure partners. This information consists of malicious cyber actors' tactics, techniques, procedures (TTPs) and associated indicators, to assist in network defense capabilities and planning. In addition, Treasury occasionally receives information on malicious cyber actors' TTPs and associated indicators from the financial sector and continued to do so during the current reporting period.

²² Treasury's cyber security information sharing initiatives to provide certain cybersecurity threat information to the financial services sector are, pursuant to Presidential Policy Directive (PPD) 21, which preceded the EO. In PPD-21, the President outlined the national effort to strengthen and maintain secure, functioning, and resilient critical infrastructure, which provides the essential services that underpin American society. PPD-21 designated the financial services sector as a critical infrastructure sector and designated Treasury as the SSA for the financial services sector. Treasury, in coordination with the Department of Homeland Security and other relevant federal departments and agencies, is responsible for providing, supporting, and facilitating technical assistance for this sector to identify vulnerabilities and help mitigate incidents, as appropriate. However, these activities are within the scope of the EO, therefore, it is included as part of this report.

OCIP shares cyber threat information in the form of unclassified Cyber Intelligence Group (CIG)²³ Circulars, through monthly meetings, and upon request from the financial services sector or a member of the sector. These activities are described in more detail below:

CIG Circulars and Financial Services Sector Requests

OCIP's CIG Circulars are intended to increase the volume, timeliness and quality of cyber threat information shared with the U.S. financial services sector so that sector entities may better protect and defend themselves against cyber threats. Pursuant to EO 13636 and the instructions issued by the Attorney General, the Secretary of Homeland Security, and the Director of National Intelligence, the U.S. Government produces timely unclassified reports of cyber threats to the U.S. homeland. In addition to these unclassified reports, the financial services sector seeks relevant information from OCIP regarding cyber threats to the financial services sector.

Specifically, OCIP receives requests for cyber threat information targeting the financial services sector through the Financial Services Information and Analysis Center (FS-ISAC). The FS-ISAC was established in 1999 pursuant to PDD 63, as an information sharing mechanism to gather, analyze, "sanitize," and disseminate information between the U.S. Government and the private sector. The FS-ISAC allows the U.S. Government to convey information to the private sector that will allow financial services firms to better protect their computer systems from attack.

The FS-ISAC makes periodic requests to Treasury for cyber threat information targeting financial sector firms that is not otherwise available to the financial sector. These requests may themselves contain cyber threat information the FS-ISAC received from private financial services sector firms, including malicious cyber actors' tactics, techniques, and procedures (TTPs) and associated indicators. As discussed above, the FS-ISAC serves as a mechanism to appropriately sanitize²⁴ information shared with the U.S. Government by the private sector.

In response to these requests, OCIP gathers declassified cyber threat information from U.S. Government sources, primarily intelligence and law enforcement agencies, to describe cyber threats to the financial services sector. OCIP uses this information to draft unclassified CIG Circulars for the purpose of sharing this cyber threat information with financial services sector entities and other critical infrastructure partners through the FS-ISAC. The information obtained by OCIP is lawfully collected by other U.S. Government agencies and only includes information approved for release by the U.S. Government data owner or owners to the FS-ISAC, for network defense purposes. OCIP does not solicit information from the private sector for inclusion in the

²³ The CIG consists of a specialized team of analysts with expertise in financial services, cybersecurity, and intelligence analysis. The CIG's primary function is to distribute timely and actionable information and analysis that financial institutions can use to protect themselves from cyber attacks.

²⁴ The term "sanitization," includes (but is not limited to) distilling the information so it is not traceable to the submitter and does not reveal any information that:

- Is proprietary, business-sensitive, or a trade secret;
- Relates specifically to the submitting person or entity (explicitly or implicitly); or
- Is otherwise not customarily in the public domain.

CIG Circulars. In one instance during the FY 2015 reporting period, Treasury included information supplied by a private sector entity through FS-ISAC in a produced CIG Circular.

OCIP shares cyber threat information in the form of unclassified CIG Circulars, and upon request from the financial services sector or a member of the sector. CIG Circulars provide information on advanced persistent cyber threat actors' tactics, techniques and procedures and associated indicators. CIG Circulars are provided to financial institutions, their supporting cyber security service providers, financial regulators, DHS's Cyber Information Sharing and Collaboration Program, and other critical infrastructure partners, for the purpose of protecting U.S. critical infrastructure from cyber threats.

Monthly Classified Cyber Information Meetings

To increase the volume, timeliness, and quality of cyber threat information shared with U.S. financial sector entities, in FY 2015, Treasury's Financial Sector Cyber Intelligence Group (CIG) began holding monthly classified cyber information meetings for cleared financial sector representatives and, separately, for cleared financial regulators. The meeting participants have to provide the following PII to enter the Treasury building: legal name, date of birth, social security number, and nationality. This information is also needed to verify that the participants have active security clearances. Instead of providing their PII each month, Treasury gave the meeting participants the option of authorizing the CIG, in writing, to retain their PII to facilitate building access and clearance verification for CIG-sponsored meetings in 2015. With their permission, their PII is stored in a locked cabinet in a Sensitive Compartmented Information Facility (SCIF) in a folder marked Privacy Protected Data. In particular, the CIG retains the PII for 11 cleared financial sector representatives, 19 cleared financial regulators, and six FBI and DHS personnel to facilitate their participation in the meetings. The participants have the option of authorizing the CIG to retain their PII to facilitate building access and clearance verification for CIG-sponsored meetings in 2016. If they choose to not authorize the CIG to retain their PII in 2016, their PII will be destroyed.

Cyber Security Information Sharing PCL Assessment

PIAs or Other Documentation

Information in this program is disseminated through correspondence and uploaded onto two portals: the Financial Services Information Sharing and Analysis Center (FS-ISAC) portal, and the DHS HSIN Financial Services portal, which is maintained by Treasury. Treasury's non-classified electronic correspondence and shared drives are maintained on the DO LAN. All Treasury information systems used to process and store PII undergo a mandatory SA&A process to verify that the system provides adequate measures to preserve the confidentiality, integrity, and availability of all sensitive information residing on or transiting those systems. A PIA is not required when information contained in a system relates to internal government operations or when it has been previously assessed under an evaluation similar to a PIA.

Standard for Sharing PII

OMB Memorandum 07-16 defines personally identifiable information (PII) 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.”

OCIP only intends to produce technical descriptions of malware in its CIG Circulars. The CIG Circulars produced for the FS-ISAC in FY 2015 described cyber threats to the financial services sector, including technical information that would help a network systems administrator identify a particular form of malware rather than an individual. They did not include any individual’s name, Social Security number, biometrics, or e-mail address. Some of the technical descriptors included in the CIG Circulars may include TTPs, file names, domain names, and Internet Protocol (IP) addresses to which malware beacons direct, or hashes that characterize particular forms of malware. In some cases, these technical descriptions could be PII under OMB’s broad definition because they potentially could link back to an individual. IP addresses, for example, sometimes could be traced back to entities, groups of individuals sharing an IP address, or a specific individual. OCIP, however, does not “link” an IP address or other technical description back to a particular entity, group, or individual, even if it were possible to do so in certain cases. OCIP only uses the technical descriptions to alert the financial services sector to a characteristic of a particular piece of malware, not to identify a specific individual or entity.

Although any PII associated with technical descriptions in CIG Circulars is *de minimis*, Treasury nevertheless analyzed the contents of the circulars to assess compliance with the FIPPs. OCIP includes technical descriptions in its CIG Circulars when they are relevant and necessary to describe a cyber threat to the financial services sector. CIG Circulars report information that is actionable, relevant, timely, and not available elsewhere to the financial sector. When responding to specific requests for information from the FS-ISAC, OCIP only requests lawfully obtained information from U.S. Government intelligence community and law enforcement agencies to address the request. All information included in CIG Circulars is declassified and approved for release to the FS-ISAC by the data owner or owners.

The CIG Circulars are produced for the FS-ISAC pursuant to the Traffic Light Protocol (TLP) initially established by DHS and adopted with modifications by the FS-ISAC. Most of the CIG Circulars are identified as TLP Green, which permits sharing among peers, trusted government and critical infrastructure partners, and service providers, but not via publicly accessible channels. FS-ISAC explains the TLP to its members. FS-ISAC distributes the Circulars to critical infrastructure owners in other sectors through the National Council of ISACs and also to members of the DHS Homeland Security Information Network (HSIN) Financial Services Portal. Treasury shares the information obtained through its cyber security activities for cybersecurity purposes only.

FIPPS and Civil Liberties Analysis:

| Transparency: | Response: |
|--|---|
| How is the general public informed about this program? | The general public is informed of this program through PDD 21 and through this report. |
| Does the agency operate a Privacy Act system of records in support of this program? | The information sharing process does not require a system of records notice because PII is not collected by Treasury directly, but relies upon Intelligence and Law Enforcement agencies to collect and identify cyber threat information. Treasury then requests from the collecting agency the permission to disseminate that cyber threat information to the financial sector. Potential cyber security threats, as well as technical indicators and tactics, techniques, and procedures of known cyber threats are distributed in this program to prevent cybersecurity attacks on the financial services sector. |

| Individual Participation: | Response: |
|--|--|
| Are individuals asked for consent and given the opportunity to object to the collection of their PII? | <p>Treasury is not responsible for the collection of PII in this program and therefore is not required to ask for consent.</p> <p>The CIG Circulars produced to the FS-ISAC in FY 2015 described cyber threats to the financial services sector, including technical information that would help a network systems administrator identify a particular form of malware rather than an individual. In some cases, these technical descriptions could be PII under OMB’s broad definition, because they potentially could link back to an individual. However, Treasury does not “link” the technical descriptions back to a particular entity, group, or individual, even if it were possible to do so in certain cases. Therefore, it would be impossible for Treasury to obtain consent from individuals who may be linked to the technical information included in CIG Circulars, and in the monthly meetings.</p> |
| Are individuals given the opportunity to access and correct their PII? | The information is related to cyber threats, not individuals, and is collected by intelligence agencies and law enforcement, who have their own processes and procedures for handling and correcting PII. |
| Describe the mechanism provided for an individual to seek redress in the event of inappropriate access to or disclosure of their PII. | If inappropriate access or disclosure gave rise to sufficient risk to the individual or Treasury, Treasury would provide notification to the individual as required in TD 25-08, <i>Safeguarding Against and Responding to the Breach of PII</i> . If notification is given under TD 25-08, a relevant point of contact would be given, to whom questions may be directed. If questions evolve into a complaint, the complaint will be |

| | |
|--|--|
| | addressed by the Office of Privacy, Transparency, and Records. |
|--|--|

| | |
|--|--|
| Purpose Specification: | Response: |
| Please provide the specific purpose(s) for the maintenance of PII within the system | Intelligence and law enforcement agencies gather information regarding cyber threat information, which may contain limited PII in the form of IP addresses. As part of its information sharing activities under PPD 21 and Section 4 of EO 131636, Treasury expressly requests declassification of cyber threat information for dissemination to the Financial Services Sector to assist with network defense. |

| | |
|--|---|
| Data Minimization: | Response: |
| Please describe the data elements that are relevant and necessary. | <p>Treasury does not collect information directly, but relies upon Intelligence and Law Enforcement agencies to collect and report cyber threat information. Treasury then requests from the collecting agency the permission to disseminate that cyber threat information to the financial sector. Potential cyber security threats, as well as technical indicators and tactics, techniques, and procedures of known cyber threats are distributed in this program to prevent cybersecurity attacks on the financial services sector.</p> <p>The CIG Circulars produced for the FS-ISAC in FY 2015 described cyber threats to the financial services sector, including technical information that would help a network systems administrator identify a particular form of malware rather than an individual. They did not include any individual’s name, Social Security number, biometrics, or e-mail address. Some of the technical descriptors included in the CIG Circulars may include TTPs, file names, domain names, and IP addresses to which malware beacons direct, or hashes that characterize particular forms of malware.</p> <p>OCIP along with Treasury’s Office of Privacy Transparency and Records has determined that the de minimis PII that may be linked to the TTPs, file names, domain names, IP addresses to which malware beacons direct, or hashes from CIG Circulars are relevant and necessary to describe a cyber threat to the financial services sector.</p> <p>CIG Circulars report information that is actionable, relevant, timely, and not available elsewhere to the financial sector.</p> |
| How long does Treasury retain the information contained in CIG Circulars? | Treasury does not limit recipients’ retention of the information contained in CIG Circulars. OCIP presently keeps copies of all its Circulars for reference purposes; the |

| | |
|--|--|
| | <p>oldest CIG Circular derived from law enforcement reporting was issued on December 2, 2013. Treasury will continue to evaluate the appropriate retention schedule for cyber threat information and will develop a more definite retention schedule as the program continues.</p> |
|--|--|

| Use Limitation: | Response: |
|--|--|
| <p>Please describe the steps taken to ensure the use of PII is limited to the purpose(s) specified in applicable notices.</p> | <p>Treasury only shares cyber security information for cyber security purposes. OCIP shares information that is actionable, relevant, timely and not available elsewhere to the financial sector. When responding to specific requests for information from the FS-ISAC, OCIP only requests lawfully obtained information from U.S. Government intelligence community and law enforcement agencies to address the request. All information included in CIG Circulars is declassified and approved for release to the FS-ISAC by the data owner or owners. In the event PII were to be included in the CIG Circulars, the inclusion of the PII in the CIG Circulars would be assessed by Treasury as relevant and necessary to describe a cyber threat to the financial services sector.</p> <p>The CIG Circulars are produced to the FS-ISAC pursuant to the TLP²⁵ initially established by the U.S. Department of Homeland Security and adopted with modifications by the FS-ISAC. Most of the CIG Circulars are identified as TLP Green, which permits sharing between peers, trusted government and critical infrastructure partners, and service providers, but not via publicly accessible channels. FS-ISAC explains the Traffic Light Protocol to its members. FS-ISAC distributes the Circulars to critical infrastructure owners in other sectors through the National Council of ISACs and also to members of the DHS Homeland Security Information Network (HSIN) Financial Services Portal.</p> |

²⁵ For more information on the TLP, see: <https://www.us-cert.gov/tlp>.

| Data Quality and Integrity: | Response: |
|---|---|
| What steps are taken to ensure the continued quality and integrity of data maintained by the project or system? | Treasury relies heavily on the accuracy of the information provided by the Law Enforcement and Intelligence Agencies. The information obtained by OCIP is lawfully collected by other U.S. government agencies and only includes information approved for release by the U.S. government data owner or owners to the FS-ISAC, for network defense purposes. |
| What steps are taken to ensure information maintained in the system is accurate, timely, relevant, and complete? | Treasury relies heavily on the accuracy of the information provided by the Law Enforcement and Intelligence Agencies. The information obtained by OCIP is lawfully collected by other U.S. government agencies and only includes information approved for release by the U.S. government data owner or owners to the FS-ISAC, for network defense purposes. |
| Please describe the method for eliminating PII that is no longer needed. | Treasury’s Office of Privacy, Transparency, and Records reviews OCIP CIG Circulars and has yet to specifically identify PII in CIG Circulars. PTR will continue to review CIG Circulars to identify PII and work with OCIP to ensure that unnecessary PII is eliminated. |

| Security: | Response: |
|--|--|
| If data from the system is sent electronically, what methods are in place to ensure appropriate safeguards apply? | The information is distributed to the financial sector and other critical infrastructure partners by electronic means. The dissemination is limited by the Traffic Light Protocol ²⁶ and includes a statement that the information is “NOT FOR POSTING ON ANY PUBLIC-FACING WEBSITE.” |

| Accountability and Auditing: | Response: |
|--|--|
| Please describe any agency oversight mechanisms that apply to the system. | PTR works with OCIP to review CIG Circulars that are released to the financial services sector. This provides a layer of oversight for the potential sharing of PII. |

²⁶ For more information on the TLP, see: <https://www.us-cert.gov/tlp>.

| |
|---|
| Civil Liberties Considerations: |
| The Office of Privacy, Transparency, and Records reviewed this activity, its standards and the criteria for participation in it, and found no significant civil liberties issues requiring discussion and assessment at this time. |

PCL Risks and Recommendations

| Risk: | Impact: |
|--|---|
| Please explain the risk associated with the accuracy of the information. | As the distributor of this information, Treasury risks distributing inaccurate information from other agencies in this program. Without a way to verify information, Treasury is at risk of providing inaccurate information to the private sector. Any distributed inaccurate information could potentially have negative impacts on the effectiveness of cybersecurity in the private sector. |
| Please describe risk that Treasury is retaining information for a longer period than necessary. | There is a risk that Treasury’s retention of information shared for cyber security purposes is not limited. Treasury is working to develop an appropriate retention schedule that will ensure that the information, and potential PII shared in the program is not retained for a longer period than necessary. |

Cyber Security Information Sharing Summary

Treasury has conducted its review for the reporting period and has determined that the limited role the Department plays in the Cyber Security Information Sharing raises no broader PCL issues, policy considerations, nor legal considerations. Treasury will continue to evaluate its role in the program and may develop a more thorough privacy assessment, as that role expands or changes for future reports.

Detailed Analyses of Identification of Critical Infrastructure at Greatest Risk under Sec. 9 of EO 13636

Section 9. Identification of Critical Infrastructure at Greatest Risk: *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.*

Heads of Sector-Specific Agencies and other relevant agencies shall provide the Secretary with information necessary to carry out the responsibilities under this section. 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 does not collect or disseminate PII in this program. Therefore, an analysis of the privacy and civil liberties concerns of this program at Treasury is not necessary.

Conclusion

Treasury continues to play a minor role in the distribution information to the financial services sector. Treasury will continue to assist in the sharing of cybersecurity information while protecting privacy and civil liberties. If Treasury's role expands or the Department substantially changes its activities under the order, we will provide a comprehensive privacy and civil liberties assessment of those activities in future reports.

PART III: DEPARTMENT OF DEFENSE



2016 EO 13636 Privacy & Civil Liberties Assessment Report

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

Dear Ms. Neuman:

I write as the Department of Defense (DoD) Privacy and Civil Liberties Officer. Pursuant to the requirements of Section 5 of Executive Order (EO) 13636, “Improving Critical Infrastructure Cybersecurity”²⁷ and Presidential Policy Directive 21 (PPD-21), “Critical Infrastructure Security and Resilience,”²⁸ this letter supplements DoD’s privacy and civil liberties assessments of the Defense Industrial Base (DIB) Cybersecurity/Information Assurance (CS/IA) Program contained in the 2014 and 2015 EO 13636 Privacy and Civil Liberties Assessment reports.

For the 2016 report, the DoD decided against replicating its 2014 and 2015 privacy and civil liberties assessments because the DIB CS/IA Program policies and procedures have not materially changed. Instead, this letter briefly summarizes DIB CS/IA Program activities that were carried out during Fiscal Year (FY) 2015, October 1, 2014 through September 30, 2015, in accordance with privacy and civil liberties safeguards.

EO 13636 establishes policy directing the U.S. Federal Government to work together with U.S. private sector entities to strengthen the security and resilience of the Nation’s critical infrastructure against cyber threats. Section 5 requires senior agency officials for privacy and civil liberties to incorporate privacy and civil liberties protections into such activities, to conduct assessments of those activities, and submit the assessments to the Department of Homeland Security for compilation and publication of a public report. Section 5(b) adds that the report shall be reviewed on an annual basis and revised as necessary.

The DoD’s privacy and civil liberties assessment focuses on the activities of the DIB CS/IA Program. The DIB encompasses the DoD, U.S. Federal 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. PPD-21 designates the DoD as the Sector-Specific Agency (SSA) for the DIB. The DoD established the DIB CS/IA Program to enhance and supplement DIB capabilities to safeguard DoD information that resides on, or transits, DIB unclassified information systems. Cyber incident reporting and related activities under this program allow the DoD to assess 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 agree to share cyber threat information out of a mutual concern for the protection of sensitive, but unclassified information, related to DoD programs on DIB company networks. Through collaboration and information sharing under this program, DoD and DIB participants increase cyber situational awareness and capabilities to counter malicious cyber activity.

²⁷ Available at <https://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf>.

²⁸ Available at <https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>.

As noted above, the structure and activities of the DIB CS/IA Program have not materially changed since DoD's submissions to the 2014 and 2015 reports. DoD's submission to the 2014 report²⁹ assessed the activities of the DIB CS/IA Program based upon the Fair Information Practice Principles (FIPPs). For the 2015 report³⁰, DoD enhanced its privacy and civil liberties assessment of the DIB CS/IA Program by incorporating constructive feedback and suggestions provided by the Privacy and Civil Liberties Oversight Board. Both assessments concluded that the DIB CS/IA Program protects our Nation's critical infrastructure from cyber threats in a manner that preserves individual privacy and civil liberties.

In FY 2015, the DoD expanded industry participation in the DIB CS/IA Program to 128 companies. Each of these participating DIB companies agreed to protect individual privacy and civil liberties before reporting any cyber incidents discovered on its networks that resulted in an actual or potential compromise of DoD information. This voluntary agreement includes compliance with Title 32 of the U.S. Code of Federal Regulations (CFR), Part 236, "Department of Defense (DoD) – Defense Industrial Base (DIB) Voluntary Cyber Security and Information Assurance (CS/IA) Activities."³¹ 32 CFR Part 236 places responsibility on DoD and each DIB company to conduct DIB CS/IA Program activities in accordance with applicable laws and regulations, including restrictions on the interception, monitoring, access, use, and disclosure of electronic communications or data. 32 CFR Part 236 also requires the DIB company to perform a legal review of its policies and practices that support its program activities before sharing any information with the Government.

Additionally, the DoD began updating DIB CS/IA Program documentation in FY 2015 to increase transparency about how DoD and DIB companies maintain personally identifiable information (PII) in electronic form, including PII embedded in information shared for cyber security analysis. Specifically, the DoD reviewed the Privacy Impact Assessment (PIA) for the DIB Cybersecurity Activities³² and the System of Records Notice (SORN) for the DIB Cybersecurity (CS) Activities Records³³ to ensure that adequate privacy safeguards exist for all information maintained by the DIB CS/IA Program. This review verified the legal authority for collecting and storing DIB CS/IA Program records, the individuals about whom the records are collected, the type of information collected, and how the records are used. The DoD published updates to both documents in FY 2016 and will include details of the revisions in its submission to the 2017 report.

²⁹ Available at <http://www.dhs.gov/publication/executive-order-13636-privacy-and-civil-liberties-assessment-report-2014>.

³⁰ Available at <http://www.dhs.gov/publication/2015-executive-order-13636-privacy-and-civil-liberties-assessment-report>.

³¹ Available at <http://www.gpo.gov/fdsys/pkg/CFR-2013-title32-vol2/pdf/CFR-2013-title32-vol2-part236.pdf>.

³² Available at http://dodcio.defense.gov/Portals/0/Documents/DIB%20CS-IA%20PIA_FINAL_signed_30jun2011_VMSS_GGMR_RC.pdf.

³³ Available at

<http://dpcl.d.defense.gov/Privacy/SORNsIndex/DODwideSORNArticleView/tabid/6797/Article/570553/dcio-01.aspx>.

The voluntary reporting under the DIB CS/IA Program focuses on sharing cyber threat indicators that participating DIB companies believe are valuable in alerting the Government and other DIB CS/IA Program participants, as appropriate, to better counter threat activity. It does not replace or duplicate mandatory reporting required by law, regulation, policy, or contractual obligations. This includes mandatory reporting requirements under Section 941 of the National Defense Authorization Act (NDAA) for FY 2013 and Section 1632 of the NDAA for FY 2015³⁴, which require defense contractors to report successful penetrations of covered contractor networks that affect or have the potential to affect covered defense information, or incidents that affect a contractor's ability to provide operationally critical support.

The NDAA's mandatory reporting requirements for defense contractors are levied at DoD in contractual language. DoD implements the requirements through Defense Acquisition Regulations System (DFARS) Case 2013-D018, "Network Penetration Reporting and Contracting for Cloud Services", published as an interim rule on August 26, 2015.³⁵ This rule establishes the same processes and systems for mandatory cyber incident reporting that already exist for voluntary reporting under the DIB CS/IA Program, and requires defense contractors to rapidly report successful penetrations of their unclassified networks or information systems while also ensuring that privacy and civil liberties protections continue to be effective.

Overall, the DIB CS/IA Program's privacy and civil liberties framework provides a multi-layered approach to the incorporation of the FIPPs, as well as other privacy and civil liberties protections guaranteed by Federal law and DoD regulations, policies, and procedures. The activities of the DIB CS/IA Program in FY 2015 complied with these privacy and civil liberties safeguards. In FY 2016, DoD will continue to monitor the DIB CS/IA Program to ensure that all privacy and civil liberties controls are functioning properly.

Sincerely,

Peter Levine
DoD Privacy and Civil Liberties Officer

³⁴ Sections 941 and 1632 are codified in Sections 391 and 393 of Title 10, United States Code. Available at <http://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title10-chapter19&saved=|KHRpdGxIOjEwIHNIY3Rpb246MzIxIGVkaXRpb246cHJlGltKQ%3D%3D||1|false|prelim&edition=prelim>.

³⁵ Available at <https://www.federalregister.gov/articles/2015/08/26/2015-20870/defense-federal-acquisition-regulation-supplement-network-penetration-reporting-and-contracting-for>.

PART IV: DEPARTMENT OF JUSTICE



I. Introduction

Executive Order (“EO” or “Executive Order”) 13636 aims to strengthen the cybersecurity of critical infrastructure by increasing information sharing, and by jointly developing and implementing a framework of cybersecurity practices with industry partners.³⁶ The EO requires agencies to coordinate their activities under the EO with their Senior Agency Officials for Privacy and Civil Liberties (SAOPCL), and to ensure that privacy and civil liberties protections are incorporated into such activities based upon the Fair Information Practice Principles (FIPPs) and other privacy and civil liberties policies, principles, and frameworks. Annually, the SAOPCLs are to provide written assessments of agencies’ activities under the EO to the Department of Homeland Security (DHS) for consideration and inclusion in a government-wide report compiled by the DHS Privacy Office and Office for Civil Rights and Civil Liberties.

The Department of Justice (“DOJ” or “the Department”) submitted privacy and civil liberties assessments for inclusion in the 2014 and 2015 government-wide reports. Both assessments detailed the Department’s activities implementing Section 4(a) and Section 4(b) of the EO. In addition, the 2015 assessment included a description of the Department’s privacy and civil liberties framework, as well as the Department’s cybersecurity framework. The Department engages in cybersecurity information sharing under the EO through activities undertaken by the Federal Bureau of Investigation (FBI). Accordingly, the 2015 assessment included descriptions of FBI-specific frameworks and protections for privacy and civil liberties, as well as detailed assessments of two FBI activities that, although not undertaken specifically pursuant to EO 13636, align with the goals of the EO.³⁷ This assessment covers the timeframe from October 1, 2014 to September 30, 2015.

II. Implementation of Section 4(a)

Section 4(a) of EO 13636 establishes as the policy of the U.S. Government the requirement 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. Section 4(a) also requires the DHS Secretary, the Attorney General (AG), and the Director of National Intelligence (DNI) to issue instructions to ensure the timely production of unclassified cyber threats to the U.S. homeland that identify a specific targeted entity (“cyber threat reports”). The instructions are to address the need to protect intelligence and law enforcement sources, methods, operations, and investigations.

As noted in the Department’s 2014 assessment, the Office of the Deputy Attorney General (ODAG) issued a Department Order requiring the timely production of unclassified reports of cyber threats to the U.S. homeland that identify a specific targeted entity.³⁸ The Order also requires that all actions taken pursuant to the Order must be consistent with the need to protect privacy and

³⁶ 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>.

³⁷ These two activities, iGuardian and Malware Investigator, were assessed in detail in the 2015 report and will not be further elaborated upon in this assessment. As noted in the 2015 report, these activities do not fall within the scope of EO 13636. This report focuses on Cyber Guardian, which implements Section 4(b) of EO 13636.

³⁸ DOJ Order 3393, Issuing Instructions Pursuant to Executive Order 13636 Regarding the Timely Production of Unclassified Reports of Cyber Threat Information (2013).

civil liberties. The implementation of Section 4(b), discussed below, addresses the plan of the United States government to address sharing cyber threat information with the private sector by coordinating the interagency management of cyber threats and the ultimate notification to specific targeted entities.

III. Implementation of Section 4(b)

Under Section 4(b) of EO 13636, the DHS Secretary and the AG, in coordination with the DNI, are required to establish a process that rapidly disseminates cyber threat reports to the targeted entity. Such a process shall also, consistent with the need to protect national security information, include the dissemination of classified reports to critical infrastructure entities authorized to receive them. Finally, Section 4(b) of EO 13636 requires the DHS Secretary and the AG, in coordination with the DNI, to establish a system to track the production, dissemination, and disposition of these reports, the so-called “4(b) solution.”

The Department’s 2015 assessment described the initial interagency efforts to develop the 4(b) solution, including the establishment of an interagency Joint Requirements Team (JRT), with guidance from the White House’s National Security Council (NSC). The JRT, with representatives from FBI, DOJ, DHS, Defense Cyber Crime Center (DC3), Defense Security Service (DSS), National Security Agency, and Sector Specific Agencies (SSAs) and other government agencies/components interested in participating in the targeted entity notification requirements and development process, developed and finalized a document titled, “Executive Order (EO) 13636 Section 4(b) Support Capability Requirements for Notification to Critical Infrastructure Targeted Entities” (accepted April 10, 2015). This document was used as the starting point for the development of the requirements for the 4(b) process and to build an agreed-upon business process and technical solution to implement the 4(b) solution. On April 10, 2015, the NSC, through the Cyber Interagency Policy Committee, authorized the FBI’s National Cyber Investigative Joint Task Force (NCIJTF) to implement Section 4(b) of EO 13636 through the use of Cyber Guardian, a sharing and integration platform. Thus, Cyber Guardian is being developed and implemented by an interagency effort as the 4(b) solution and will be modified, as appropriate, as additional requirements are identified.

The FBI conducted a Privacy Impact Assessment (PIA) on Cyber Guardian that assessed the privacy risks in accordance with Section 208 of the E-Government Act of 2002,³⁹ the Office of Management and Budget directives, DOJ policy, and specific FBI guidance.⁴⁰ Each of these requirements incorporates the FIPPs (*e.g.*, transparency; individual participation; purpose specification; data minimization; use limitation; data quality and integrity; security; and accountability and auditing) in assessing how privacy and other protections are incorporated into Cyber Guardian. A FIPPs assessment of Cyber Guardian is included as Attachment A.

Cyber Guardian currently serves as the tracking system for the production, dissemination, and disposition of cyber threat reports from the U.S. Government that are shared with U.S. private

³⁹ See 44 U.S.C. § 3501 (note) (2012).

⁴⁰ The PIA was completed by FBI and is currently under review by DOJ Office of Privacy and Civil Liberties.

sector entities. Cyber Guardian offers Federal Cyber Centers⁴¹ and Intelligence Community (IC) partners the ability to coordinate a whole-of-government response to targeted entities and victims of cyber incidents identified in government intelligence collections. The FBI is currently in the process of making Cyber Guardian available to all Cyber Centers, designated SSAs, and other government agencies that directly support the cybersecurity mission by providing direct access through the SIPRNet⁴² Intelink-S connection from their home agencies. This will provide a foundation for strengthening the defenses of all participating agencies by allowing use of a universal application for near real-time coordination and collaboration of all cyber targeted entity notifications that meet the appropriate cyber incident severity threshold.

Today, Cyber Guardian enables government agencies with cyber missions to be aware of and de-conflict cyber incidents. In the future, Cyber Guardian will be a platform for threat reports to be assimilated and made available for dissemination to the private sector, and is intended to have the capability to disseminate both unclassified and classified reports to critical infrastructure entities authorized to receive them. Any new capability, if developed, will be assessed for privacy and civil liberties protections, and the PIA will be amended as necessary.

To gain access to the Cyber Guardian system, each agency and each individual designated to receive access to Cyber Guardian from such agency, as appropriate, must undertake the following:

- Complete on-site Cyber Guardian training;
- Review, sign, and return the FBI Rules of Behavior for Other Government Agency (OGA) Personnel Authorized to Access Cyber Guardian (FD-889d);
- Possess and provide a valid Intelink Passport account (if accessing through SIPRNet); and
- Obtain Agency Head authorization and signature on FBI's Memorandum of Understanding (MOU) for Access to Cyber Guardian

In June 2015, the FBI initiated Phase I of its Cyber Guardian training to all designated Federal Cyber Centers, select SSAs, and other select government agencies with a cybersecurity mission. To date, the NCIJTF/CyWatch⁴³ has coordinated and provided multiple training sessions to DHS, DC3, Intelligence Community Security Coordination Center, Department of Energy, Treasury, and DSS. Also scheduled to receive training as part of Phase I are the following additional government agencies: NSA/CSS Threat Operations Center, U.S. Cyber Command, and the Central Intelligence Agency (CIA).

The FBI will continue to work with its Cyber Partners to identify new requirements for Cyber Guardian to ensure that quality cyber threat information is increasingly shared in a timely manner to targeted private entities that are victims of cyber threats so that these entities may better protect

⁴¹ Under the Enhance Shared Situational Awareness initiative, the following Federal cybersecurity centers are developing an information-sharing framework and shared situational awareness requirements, for sharing cybersecurity information: Defense Cyber Crime Center (DC3); Intelligence Community Security Coordination Center (IC-SCC); National Cybersecurity and Communications Integration Center (NCCIC); National Cyber Investigative Joint Task Force (NCIJTF); National Security Agency / Central Security Service (NSA/CSS) Threat Operations Center (NTOC); and United States Cyber Command (USCYBERCOM) Joint Operations Center (JOC)

⁴² SIPRNet (SECRET Internet Protocol Network Router) is a service gateway function that provides protected connectivity to federal, IC, and allied information at the secret level.

⁴³ The FBI's 24-hour cyber command center.

2016 EO 13636 Privacy & Civil Liberties Assessment Report

themselves from malicious cyber threats. Further, the FBI will continue to assess any modifications to Cyber Guardian that may affect privacy and civil liberties protections afforded to individuals affected by cyber threat reporting.

Attachment A

In accordance with Section 5(b) of the EO, this assessment includes an update of the activity that aligns with the EO during this reporting period against the FIPPs and other applicable privacy and civil liberties policies, principles, and frameworks. The FIPPs are instructive of the appropriate handling of personally identifiable information (PII) by the FBI’s Cyber Division (CyD) for the purpose of protecting the cybersecurity of critical infrastructure.

In addition to the FIPPs, the FBI considers other applicable privacy and civil liberties policies, principles, and frameworks. For example, this chart includes information on how the FBI adheres to federal privacy laws such as the Privacy Act of 1974 (“the Privacy Act”)⁴⁴ and Section 208 of the E-Government Act of 2002. The FBI has no indication of any activity that would warrant a separate civil liberties review. The Cyber Guardian MOU prohibits federal agencies accessing Cyber Guardian from submitting to Cyber Guardian, or retaining, disseminating, or otherwise using in connection with Cyber Guardian any information based solely on the ethnicity, race, gender, disability or religion of an individual or based solely on the exercise of rights guaranteed by the United States Constitution or the lawful exercise of any other rights secured by the laws of the United States.

Cyber Guardian FIPPs Chart

| |
|---|
| (a) Transparency |
| 1. <i>How does the FBI incorporate the principle of transparency into Cyber Guardian?</i> |
| Response: The FBI incorporates transparency into Cyber Guardian ⁴⁵ by providing notice to users (currently U.S. government agencies with cyber missions) regarding its collection, use, dissemination, and maintenance of PII via the applicable System of Records Notices (SORNs), Privacy Act Statement, electronic banner, and MOU. For Privacy Act purposes, Cyber Guardian login information is covered under Privacy Act SORN, DOJ-002, DOJ Computer Systems Activity and Access Records. ⁴⁶ Upon login, each Cyber Guardian incident receives prompt, individualized review by the FBI’s National Cyber Investigative Joint Task Force (NCIJTF)/CyWatch to determine if additional action is warranted. Any information ultimately maintained by FBI would be covered under Privacy Act SORN, FBI-002, The FBI Central Records System, 63 Fed. Reg. 8671 (Feb. 20, 1998), as amended by 66 Fed. Reg. 8425 (Jan. 31, 2001), 66 Fed. Reg. 17,200 (Mar. 29, 2001), and 72 Fed. Reg. 3410 (Jan. 25, 2007); and FBI-022, FBI Data Warehouse System, 77 Fed. Reg. 40630 (July 10, 2012). A SORN for the Guardian Prime System is presently under review by DOJ and encompasses Cyber Guardian. As Cyber Guardian develops, the FBI will continuously assess privacy and civil protections for the program and may develop a separate Cyber Guardian SORN, if warranted. Additionally, the FBI has conducted a PIA on Cyber Guardian, under review by DOJ, which assessed the privacy risks in accordance with the E-Government Act of 2002. Cyber Guardian is a National Security System, |

⁴⁴ 5 U.S.C. § 552a (2012).

⁴⁵ Cyber Guardian was developed from the Guardian system, which was created initially by the FBI to collect suspicious activity reports regarding terrorist threats and to triage, assign, and assess such information. However, the two applications are hosted on different sets of web application servers.

⁴⁶ DOJ-002, the DOJ Computer Systems Activity and Access Records SORN, available at: <https://www.gpo.gov/fdsys/pkg/FR-1999-12-30/pdf/99-33838.pdf>.

as determined by the FBI's Security Division. Constructive notice of these systems is provided by the applicable SORNs.

Before cleared U.S. government personnel of Cyber Partners are granted access to Cyber Guardian, the proposed users are provided with a comprehensive Privacy Act Statement and other detailed information related to system use, such as information regarding monitoring and auditing for security purposes. Although Cyber Guardian does not provide express notice regarding the treatment of third party information, the Cyber Partners must agree to the Cyber Guardian responsibilities, set forth in the MOU, that require submission of information that is directly relevant to the Cyber Incident submission. This helps ensure that Cyber Guardian only collects limited PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retains PII for as long as is necessary to fulfill the specified purpose(s). Pursuant to the MOU, each Cyber Partner agrees to notify each other if any erroneous information is disclosed pursuant to this program and take reasonable steps to correct such error, or if any PII is inadvertently disclosed. Moreover, determinations about the Cyber Guardian collected information are made promptly⁴⁷ so that the data can move quickly through the review process.

Further, before access to the system is granted, all authorized users will be under clear and conspicuous written notice through an electronic banner that information and data on the network may be monitored or disclosed to third parties or that the network users' communications are not private. These users can then decide if they wish to use the system or not, and decide what information they want to transmit over the government system.

All Cyber Guardian users must agree to an FBI MOU. Accordingly, each Cyber Partner must acknowledge, in writing, the need to incorporate transparency while recognizing the need to protect sensitive information, sources, and methods. Each Cyber Partner understands that information submitted to Cyber Guardian is subject to applicable federal laws, including but not limited to the Privacy Act, the Freedom of Information Act, the Federal Records Act, and discovery requirements. To the extent information exchanged as a result of the Cyber Guardian results in a request or demand for that (or related) information from FBI files pursuant to federal or state civil or criminal discovery or any other request by a third-party for FBI information, users are advised that such disclosure may only be made after consultation with, and upon approval by, the FBI, or as otherwise required by law. Cyber Guardian is committed to establishing an atmosphere of trust among its users, and this MOU promotes better data quality and integrity.

Once users are granted access to Cyber Guardian, a completed form may include the following items of information:

- (1) Submitter's contact information (such as name, phone number, and email address);
- (2) Information about submitter's organization (this includes work-related data such as name and work address);

⁴⁷ Upon identification and entry of new information, the FBI (CyWatch) immediately coordinates the information within their Operations Sections to assess investigative equities and impact of effecting notification. The FBI also utilizes the Cyber Incident Severity Schema, which was approved by the National Security Council, to assist in assessing urgency of coordination and notification.

(3) Threat observation information (such as when the threat was detected, how the threat was detected, the name of the suspected threat actor, the internet protocol (IP) address of the source of the threat, and whether the threat has been reported to another government agency);

(4) Information regarding the threat’s target or objective (such as the incident sector, the incident type, and the IP address of the target); and

(5) Information regarding damage/impact to submitter’s organization.

2. How does CyD ensure that issues surrounding transparency are re-evaluated on a periodic basis?

Response: Generally, the FBI requires all system owners to review and update privacy documentation every three years in accordance with the Federal Information Security Modernization Act of 2014⁴⁸ (FISMA) certification schedule and/or when the program changes in such a way that may raise new privacy issues. Because the system is evolving, the FBI anticipates continued oversight by the FBI’s privacy attorneys to ensure that issues surrounding transparency are appropriately addressed, and will re-evaluate whether the documentation for Cyber Guardian provides sufficient transparency.

(b) Individual Participation

3. Are victims asked for consent and given the opportunity to object to the collection of their PII?

Response: Third party direct consent of the cyber threat actor is not practicable due to the need to protect the confidentiality of the law enforcement investigation. When Cyber Guardian users submit incident reports, those users consent to the use of their own PII, such as name, phone number, email address, and work-related data. All information that is submitted into an FBI database must be consistent with civil liberties policies, including prohibitions against collecting information solely on the basis of race.⁴⁹

Cyber data, like information obtained in any other investigation, is evaluated for accuracy before use. In the law enforcement context, information is evaluated and analyzed prior to its use, including in any enforcement action involving a criminal statute. Insofar as accuracy of information is related to third party consent, the Department does not separately verify third party consent regarding the PII that may be included within the information provided by a Cyber Guardian user. However, the FBI and DHS are responsible for victim notification in accordance with applicable laws and policies.

4. How does Cyber Guardian ensure that the FBI CyD’s Victim Notification Process is implemented?

Response: Currently, Cyber Guardian’s users consist of cleared U.S. government personnel of Cyber Guardian partners. Thus, in most cases, the victim will not be the same entity as the Cyber Guardian user, but instead the submission will be on behalf of a victim. However, the FBI notifies victims in accordance with applicable laws and policies. The FBI will still need to develop steps, or may consider using the FBI’s existing Victim Notification Process to make the private sector entity aware of the magnitude of the cyber incident and share information with that entity as appropriate.

5. Are Cyber Guardian users given the opportunity to access and correct their PII?

⁴⁸ See Federal Information Security Modernization Act of 2014, Pub. L. 113-283, December 18, 2014, codified at 44 U.S.C. §§ 3551 et seq., which superseded the Federal Information Security Management Act of 2002, formerly codified at 44 U.S.C. §§ 3541 et seq.

⁴⁹ Guidance for Federal Law Enforcement Agencies regarding the Use of Race, Ethnicity, Gender, National Origin, Religion, Sexual Orientation, or Gender Identity (DOJ Use of Race Policy) (December 2014), at 2.

| |
|--|
| <p>Response: Yes. Users may access and correct their user account information. If Cyber Guardian users would like to update their submissions, users are required to make a new submission or contact the Cyber Guardian program.</p> |
| <p>6. Are victims given the opportunity to access and correct their PII?</p> |
| <p>Response: To the extent that a victim’s information is retrieved by name or other personal identifier, it would be covered under Privacy Act SORN, FBI-002, and thus the access and amendment provisions available under the Privacy Act are applicable to such information. Although FBI-002 is exempt from the access and amendment provisions of the Privacy Act, the FBI, in the interest of accurate record-keeping, may waive such exemptions on a case-by-case basis.</p> <p>Moreover, FBI-002 is not exempt from the Privacy Act’s disclosure prohibition. Therefore, if an individual’s PII were covered by the Privacy Act and is accessed or wrongly disclosed in violation of the Act, the individual may bring a lawsuit as a form of judicial redress against the Department. Victim information, in addition to the mechanisms listed above, is covered under Privacy Act SORN, FBI-002, and thus the access and amendment provisions available under the Privacy Act are applicable to such information. Even though the SORN is exempt from access and amendment under the Privacy Act, the FBI reserves the right to waive such exemptions in individual cases. In addition, redress is available for wrongful disclosures. Individuals have the right to seek judicial redress for intentional or willful disclosures of protected information, as well as for refusals to grant access or to rectify any errors contained in that information.</p> |
| <p>7. Describe the mechanism provided for an individual Cyber Guardian user to seek redress in the event of inappropriate access to, or disclosure of, their PII.</p> |
| <p>Response: System users may seek redress regarding their own contact information by contacting the Cyber Guardian program office.</p> |
| <p>8. What steps are taken to ensure information maintained in the system is accurate, timely, relevant, and complete?</p> |
| <p>Response: Cyber Guardian incidents are reviewed in coordination with federal agencies with cybersecurity missions and by an FBI CyWatch investigator to determine if the incident warrants additional action. After this de-confliction, if the incident warrants additional action by the FBI, it is assigned to the appropriate FBI entity for additional review and investigation. Cyber Guardian has robust security mechanisms, audit capabilities, and strict user access. Cyber Guardian users are required to complete on-site Cyber Guardian training; review, sign, and return the FBI Rules of Behavior for Other Government Agency (OGA) Personnel Authorized to Access Cyber Guardian (FD-889d); possess and provide a valid Intelink Passport account (if accessing through SIPRNet); and obtain Agency Head authorization and signature on FBI’s MOU for access to Cyber Guardian. As previously discussed, the FBI’s MOU notifies users that any PII submitted must be authorized, relevant, and necessary to the submission. The obligation resides with the submitters to ensure they are authorized to provide information, including relevant and necessary PII, on the Cyber Guardian submission form.</p> |
| <p>9. 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.</p> |
| <p>Response: As stated above, Cyber Guardian users are required to submit their contact information (such as name, phone number, and email address) and information about their organization (this includes work-related data such as name and work address). There may be cases where the Cyber Guardian user submits information about the particular threat actor, and</p> |

thus the submission may contain third party PII. As explained above, the information submitted will be evaluated as part of the case management process described in the Cyber Guardian PIA to ensure that the information submitted is accurate and complete.

(c) Purpose Specification

10. *Please provide the specific purpose(s) for the maintenance of PII within the system.*

Response: Cyber Guardian is a sharing and integration platform for cleared personnel of federal agencies who have a cyber mission to share cyber threat information. Cyber Guardian enables the federal government to ensure that cyber threat incidents are shared among agencies with cyber missions to facilitate sharing of cyber threat reports to targeted private sector entities in accordance with Executive Order 13636. The specific purpose for the maintenance of PII related to cyber threat information is to facilitate information sharing and to implement Section 4(b) of EO 13636 (through the use of Cyber Guardian).

Information lawfully obtained by the FBI is generally available to all authorized FBI personnel, and consequently, information may be appropriately shared and analyzed effectively to prevent and disrupt criminal and national security threats. Specifically, the Attorney General’s Guidelines for Domestic FBI Operations (AGG-DOM) “...do[es] not require that the FBI’s information gathering activities be differentially labeled as ‘criminal investigations,’ ‘national security investigations,’ or ‘foreign intelligence collections,’ or that the categories of FBI personnel who carry out investigations be segregated from each other based on the subject areas in which they operate.”⁵⁰ The FBI is authorized to collect intelligence and to conduct investigations to detect, obtain information about, and prevent and protect against federal crimes and threats to the national security and to collect foreign intelligence, as provided in the FBI Domestic Investigations and Operations Guide (DIOG) Part II.⁵¹

As a practical matter, the information submitted on the Cyber Guardian incident form relates to cyber incidents only, and would not generally be relevant to other investigative matters. Within this framework, the FBI also strictly adheres to federal and Department information sharing procedures and safeguarding the information that it maintains. For example, the FBI is governed by federal information privacy laws, such as the Privacy Act, which permits the sharing of protected information only with individual consent or under specified statutory exceptions.

Currently, FBI’s Cyber Guardian has only been used for cybersecurity purposes based on the submissions received during the reporting period. It is important to note that the FBI may also receive cybersecurity information through other channels not subject to the EO, including directly from FBI field offices.

11. *What steps are taken to ensure the authority for the collection is valid?*

Response: For initial reporting, the FBI depends on the Cyber Guardian user to ensure the collection of information submitted to the FBI is validly collected. If the FBI plans to open a case, the FBI will follow its usual case management process to ensure that the information submitted was validly collected.

(d) Use Limitation

⁵⁰ The Attorney General’s Guidelines for Domestic FBI Operations.

⁵¹ See FBI DIOG (updated November 18, 2015) (delineating protections incorporated in this report), available at [http://vault.fbi.gov/FBI Domestic Investigations and Operations Guide \(DIOG\)/fbi-domestic-investigations-and-operations-guide-diog-2011-version/](http://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20(DIOG)/fbi-domestic-investigations-and-operations-guide-diog-2011-version/).

| |
|--|
| <p>12. <i>Describe steps taken to ensure the use of PII is limited to the purpose(s) specified in applicable notices.</i></p> |
| <p>Response: To the extent that the FBI notices through analysis that the information submitted may be evidence of another crime unrelated to the purpose for the submission, the FBI follows applicable laws and policies, such as the AGG-DOM and DIOG. As previously indicated above, the FBI can share information as necessary to fulfill its law enforcement mission. The FBI, through a multilayered approach, will continue to update information sharing policies as necessary to examine the potential impact to privacy and civil liberties.</p> |
| <p>(e) <u>Data Quality and Integrity</u></p> |
| <p>13. <i>What steps are taken to ensure that data is accurate, timely, relevant, and complete?</i></p> |
| <p>Response: For cyber threat information submitted, the likelihood that the information will be inaccurate, untimely, irrelevant, or incomplete is relatively low. Much of the information submitted is expected to be technical in nature. For information submitted that may be in narrative form describing the incident, and perhaps the specific threat actor, the information must be relevant pursuant to the FBI's MOU that all Cyber Partners enter into. Moreover, the FBI will review the information in accordance with case management procedures to determine whether the information is actionable and relevant. In a typical scenario, information is determined to be relevant when there is an articulable nexus to a known or suspected cyber incident. This information is reviewed by trained CyWatch specialists. These multiple layers of checks and balances ensure that only relevant information is transferred to FBI agents.</p> |
| <p>(f) <u>Accountability and Auditing</u></p> |
| <p>14. <i>What methods are in place to audit access to records maintained within the system?</i></p> |
| <p>Response: Cyber Guardian is hosted on the FBI's Secret Enclave and monitored by the FBI. As part of FBI's security functions, audit trails and user access are to be reviewed on a regular basis. Such compliance shall include tracking logons and logoffs, creating audit logs, review of opening and closing incident reviews, and other appropriate measures. Audit records will be protected against unauthorized access, modifications, and deletion, and will be retained for a sufficient period to enable verification of compliance. As noted above, Cyber Guardian is a National Security System maintained on the Secret enclave, which is subject to strict audit and access procedures. Further, all FBI employees must complete privacy training regarding the proper use of FBI information systems.</p> |
| <p>15. <i>Describe any oversight mechanisms that apply to the system.</i></p> |
| <p>Response: Generally, the FBI requires all system owners to review and update privacy documentation every three years in accordance with the FISMA certification schedule and/or when the program changes in such a way that may raise new privacy issues. Because Cyber Guardian is still in its beginning stages, privacy attorneys are embedded at the program level and advise on the development and use of the system. As part of this advisory role, the privacy attorneys are examining whether additional oversight will be needed beyond general oversight.</p> |

PART V: DEPARTMENT OF HEALTH AND HUMAN SERVICES



Introduction:

Executive Order (EO) 13636 seeks to ensure that the national and economic security of the U.S. is secure and resilient in the face of the ever-increasing occurrence of cyber intrusions and cyber threats. The main focus of EO 13636 is the nation's critical infrastructure, which is defined in § 2, as “systems and assets, physical or virtual, [that are] so vital to the United States that the[ir] incapacity or destruction . . . would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.”

The major components of the effort to enhance our nation's cybersecurity resiliency are collaboration and information sharing across the public and private sectors, as well as establishing partnerships with the owners/operators of critical infrastructure. The Department of Health and Human Services (HHS) engages in information sharing in its capacity as Sector Specific Agency for the Healthcare and Public Health (HPH) Sector under the National Infrastructure Protection Plan. HHS maintains a partnership with approximately 150 major trade associations and companies in the HPH Sector, as well as Federal, State, Local, Tribal and Territorial agencies. However, as information is shared, agencies must coordinate their activities in order to ensure that risks to privacy and civil liberties are minimized or mitigated. HHS shares vetted and cleared cybersecurity information with Sector partners through meetings, conference presentations, webinars, teleconferences, newsletters, and an HHS-moderated page on the Homeland Security Information Network (HSIN) secure Web portal. Information that is shared is usually in the form of a finished product highlighting general threats, vulnerabilities, and/or protective measures, and often originates from Federal sources outside of HHS.

EO 13636 § 5(c) requires “the Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties of [the Department of Homeland Security (DHS) to] consult with the Privacy and Civil Liberties Oversight Board” (PCLOB) in reporting recommendations to “minimize or mitigate” the “privacy and civil liberties risks of the functions and programs” undertaken by DHS and other agencies, such as the Department of Health and Human Services (HHS), in compliance with their responsibilities under EO 13636. In addition to supplying DHS with information on its functions and programs related to privacy and civil liberties, HHS is responsible, under EO 13636 § 5, for “coordinat[ing] their activities . . . with their senior agency officials for privacy and civil liberties and ensur[ing] that privacy and civil liberties protections are incorporated into [their] activities,” which are aimed at improving the security and resilience of physical and cyber critical infrastructure. This assessment represents HHS's contribution to the publicly-available report DHS supplies annually which contains agencies' evaluations of their activities related to privacy and civil liberties.

Establishing a strong national policy related to critical infrastructure security and resilience is a shared responsibility and requires effective organization among critical infrastructure owners and operators, as well as government agencies and their partners. As part of its function under Presidential Policy Directive 21⁵², HHS was designated the Sector-Specific Agency for the

⁵² 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>.

Healthcare and Public Health Sector, as well as the Co-Sector Specific Agency for the Food and Agriculture Sector alongside the Department of Agriculture.

Summary Description of Agency Privacy and Civil Liberties (PCL) Organization and Processes

HHS assists Healthcare and Public Health Sector partners in protecting their systems from unauthorized access, exploitation, or harm by sharing cybersecurity information and best practices with government agencies and external stakeholders. Through its participation in working groups, discussions, and other activities, HHS also works to ensure that parties have open communication channels to maximize the utility of cyber threat information sharing. HHS's EO 13636 activities are not expected to have any significant impact on privacy or civil liberties. However, HHS is aware of its responsibility to analyze and mitigate risks to constitutional liberties that any of its activities may present. It partners with other organizations and working groups to propose activities and collaborate on procedures that relate to the Department's EO 13636 efforts, ensuring an overall Department-level of preparedness. HHS is striving to ensure that, however small its footprint is in counter-terrorism-related privacy and civil liberties risk management footprint, it has mechanisms in place to proactively and effectively respond to any threats to individuals' privacy and civil liberties protections that may arise.

Due to the sensitivity and risks associated with collecting, using, storing, and sharing personally identifiable information (PII), HHS works to protect PII by leveraging technologies or programs that are sensitive to those concerns. As part of the effort to mitigate risks, HHS incorporates risk management into every phase of its system and program development and will continue to do so. When HHS is charged with regulating parties that collect information about individuals, the Department is obligated to identify, analyze, and mitigate any concerns individuals may have about the impact on their privacy.

The HHS Privacy Program

Many offices across HHS share the overall privacy policy and compliance responsibilities for the Department, each with its own particular role and/or subject-matter focus. One aspect of these responsibilities is to coordinate with one another to effectuate comprehensive implementation of the Department-wide response to EO 13636. The HHS privacy program collects, assesses, and uses significant amounts of data as part of its role as the United States Government's principal agency charged with protecting the health of all Americans and providing essential human services. HHS focuses on collaborative efforts to address privacy concerns common to all information systems that are comprised of PII, working internally with Operating Divisions (OpDivs) and with external stakeholders to identify the most efficient platform for recognizing, assessing, and mitigating privacy risk. HHS will continue its current activities that focus on the protection of individuals' privacy and civil liberties, such as holding regular privacy incident response team meetings, working with OpDivs to assist them with the responses to such incidents, and collaborating with and keeping open channels of communication with other privacy officials throughout the Department with regard to policy considerations and information management. HHS continues participating in discussions, councils, and working groups with the

goal of creating and maintaining appropriate data collection, use, protection, and dissemination procedures.

Overview of Executive Order 13636 Implementation Activities to be Reviewed and Assessed

We have no significant updates from our specific assessments from last year's report; however we would like to report on the following areas of activity:

Critical Infrastructure Protection (CIP) Program:

The Healthcare and Public Health (HPH) Sector Critical Infrastructure Protection (CIP) Program leads a public and private sector partnership known as the Healthcare and Public Health Sector Critical Infrastructure Protection Partnership in protecting the essential goods, services, and functions of healthcare and public health that, if destroyed or compromised, would negatively affect the Nation. The HHS Office of the Assistant Secretary for Preparedness and Response (ASPR) has been coordinating this program for more than ten years. The CIP Program works with its partners to develop guides and checklists to prepare facilities to bounce back after a disaster; implement the National Infrastructure Protection Plan (NIPP) sector partnership and risk management framework; develop protective programs and actions to defend against, prepare for, and mitigate the consequences of a terrorist attack or other hazards; provide guidance on Healthcare and Public Health critical infrastructure protection; communicate the needs of the Healthcare and Public Health Sector throughout government; measure the sector's performance toward sector protection priorities; encourage information sharing among all sector partners; and submit sector plans and reports to DHS.

Food and Drug Administration (FDA) Medical Device Security Efforts

At the FDA, all medical devices are regulated based on risk. Moderate- and high-risk devices are generally evaluated for their safety and effectiveness before they are allowed to be sold to the public. Increasingly, these devices are designed to be wireless, Internet and network connected, which enables remarkable advances that have the potential to transform patient care. At the same time, this interconnectivity means cybersecurity risks need to be addressed.

The FDA recognizes that collaboration with the private sector is essential to enhancing medical device cybersecurity. Engaging with all of the stakeholders in the medical device ecosystem, including security researchers, is an important step toward strengthening medical device cybersecurity. White hat hackers study medical devices and systems, looking for flaws, weaknesses, or vulnerabilities that, if exploited, could cause harm. White hats work with manufacturers, regulators, and other stakeholders to safeguard patient care and privacy without putting patients at risk – by revealing flaws in a controlled setting and reporting them so they can be proactively addressed in both current and future designs. While skilled and persistent adversaries seek to harm, skilled and persistent external “white hat” protectors seek to safeguard. Distinguishing between malicious attack by adversaries and good faith effort by security researchers allows medical device manufacturers to discourage the former and derive value from the latter. The best outcomes happen when security researchers work with medical device manufacturers and federal partners in a coordinated manner to identify and help address medical

device cybersecurity concerns together. The FDA highly values the researchers' technical expertise and regards their contributions as essential to identifying medical device cybersecurity vulnerabilities, which if exploited, may result in patient harm.

Summary of Assessment Methodology

As stated in last year's report, HHS continues to consult the Code of Fair Information Practice Principles (FIPPs), as well as more recent formulations, in evaluating its privacy functions. They are a basis for the Privacy Act of 1974⁵³ and most other privacy laws and policies. The FIPPs, as well as both domestic and international privacy statutes and regulations, and federal and state policies, have been consulted whenever an HHS program or activity collects information or raises concerns involving the collection of PII. These authorities are also consulted whenever there is a deployment of technology or development of a proposed regulation that raises privacy risks for individuals.

Summary of Findings and Recommendations

We continue to engage with the HHS organizations most involved with programs potentially under the purview of EO 13636. Much of the input for this year's report is from ASPR, who is well-suited to inform the HHS Privacy Program of new issues or programs across the Department suitable for reporting here.

Conclusion

As with our initial report, PCLOB understands the HHS position that we do not have specific systems or programs that would fall under the purview of EO 13636. HHS will continue to protect the data it collects and maintain the rights and civil liberties of the individuals to whom HHS provides benefits and services. HHS looks forward to increased collaboration with its internal and external partners, and improved awareness and efficiency of HHS policies and practices.

⁵³ 5 U.S.C. § 552.

PART VI: DEPARTMENT OF ENERGY



Department of Energy
Executive Order 13636, “Improving Critical Infrastructure Cyber Security,”
Section 5 Assessment of Privacy and Civil Liberties Protections

Pursuant to the requirements of Executive Order (E.O.) 13636, Improving Critical Infrastructure Cybersecurity, this update constitutes a review of Department of Energy (DOE) Privacy and Civil Liberties activities for the period ending September 31, 2015. DOE is the sector specific agency for energy and the Smart Grid. DOE’s previous assessment was submitted on December 2, 2014, for inclusion in the consolidated 2014 Department of Homeland Security Report, consistent with the mandate of the E.O.

DOE’s Office of Electricity Delivery and Energy Reliability (OE), the lead office for the Smart Grid, in coordination with the Federal Smart Grid Task Force (Task Force), continues to work closely with Smart Grid stakeholders to protect the privacy of consumers’ customer data. As reported last year, DOE has no jurisdiction to regulate or monitor either utilities or third parties who will be collecting or using energy usage data. As such, DOE OE, in partnership with the Task Force, initiated a multi-stakeholder process to develop the Voluntary Code of Conduct (VCC) that was modeled on the Fair Information Practice Principles, a widely accepted framework of privacy principles that provides the basis for the Privacy Act of 1974 and other privacy laws and policies.

In FY2015, the Cybersecurity Risk Information Sharing Program (CRISP) continued to expand under the management of the North American Electric Reliability Corporation’s (NERC) Electricity Information Sharing and Analysis Center (E-ISAC). CRISP is a government-energy sector collaboration to facilitate the timely bi-directional sharing of classified and non-classified threat information and develop and deploy situational awareness tools to enhance the sector’s ability to identify threats and coordinate the protection of critical infrastructure. As required by contracts with Pacific Northwest National Lab, NERC is slated to conduct its first independent audit of CRISP data handling procedures.

Voluntary Code of Conduct Update

On January 12, 2015, President Obama announced the release of the VCC final concepts and principles related to the privacy of customer energy usage data for utilities and third parties. The final concepts and principles were developed through a 22-month multi-stakeholder effort that was facilitated by OE in coordination with the Task Force. The VCC reflects input from stakeholders across the electricity industry and incorporates comments from the public through open meetings and a federal register notice. The VCC was rebranded as DataGuard|Energy Data Privacy Program in early 2015 based on feedback from consumer focus groups. Below is a summary of activities for the rebranded program:

- A consumer-friendly mark was developed that provides adopting companies a visible means for communicating their adoption of the program and demonstrating their commitment to consumer privacy. DOE filed a trademark application for the DataGuard mark and is awaiting final approval.

2016 EO 13636 Privacy & Civil Liberties Assessment Report

- Currently, 15 companies (7 utilities and 8 technology companies) have pledged to adopt DataGuard concepts and principles. Upon receipt of the trademark approval, a program launch event will take place with early adopters to highlight their leadership in this area and to raise awareness of the program. DOE OE will continue outreach efforts to recruit early adopters and raise program awareness.
- A program website was developed with both industry and consumer sections. It provides information on the program and its principles, and also serves as a public method for communicating which companies participate in the program. The industry section provides additional information on the importance of adopting and how to adopt, as well as a toolkit with communication materials that a company could use to explain the program to consumers or employees. Communication materials include a program fact sheet, newsletter and bill insert examples, website buttons, and sample press release content. In addition, a video targeting potential adopters was created which explains the program and the importance of protecting consumer privacy.

Federal Smart Grid Task Force website:

<http://energy.gov/oe/technology-development/smart-grid/federal-smart-grid-task-force>

DataGuard|Energy Data Privacy Program website:

https://www.smartgrid.gov/data_guard.html

PART VII: OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE



2016 EO 13636 Privacy & Civil Liberties Assessment Report

January 22, 2016

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

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

Dear Ms. Neuman and Ms. Mack:

I write as the Civil Liberties Protection Officer and the senior agency official for privacy and civil liberties of the Office of the Director of National Intelligence (ODNI). Pursuant to the requirements of Executive Order (EO) 13636 (February 12, 2013), Improving Critical Infrastructure Cybersecurity, this letter constitutes my review of ODNI's cyber activities for the period ending September 30, 2015.¹

Under the EO, ODNI is responsible for developing and disseminating guidance to the Intelligence Community (IC) for timely production of unclassified cyber products involving a specific, identifiable, target individual or entity. ODNI determined that the existing Intelligence Community Directive (ICD) 209, "Tearline Production and Dissemination," satisfied this requirement. We nonetheless recommended that appropriate training be developed and, in our last submission, noted that ODNI CLPO in fact had completed an online training module suitable for that purpose. The Web-based training module (including a "knowledge check") is now a mandated annual requirement for ODNI intelligence personnel, linked to system access for some purposes. The training addresses the requirements of the Privacy Act and the proper handling of personally identifiable information (PII), as well as safeguards for "protected" individuals in the Information Sharing Environment (ISE). The training is applicable to the production and dissemination of tearlines.²

¹ This is our third review under EO 13636. Our first assessment was submitted on December 2, 2013 for inclusion in the first Department of Homeland Security (DHS) Cyber Report, published in April 2014. In that initial submission, we included a comprehensive assessment of the ODNI's cyber activities under EO 13636. On February 13, 2015, we submitted our second review covering the period ending September 30, 2014 for inclusion in the second DHS Cyber Report, published in April 2015. In that second review, we did not resubmit the detailed civil liberties and privacy analysis that we had included in our first assessment, and instead focused on relevant updates. In this review, we again focus on relevant updates. For those interested in the original comprehensive assessment, please see the first DHS Cyber Report dated April 2014.

² Moreover, ODNI is implementing training on the protections for non-U.S. persons as prescribed by Presidential Policy Directive 28: Signals Intelligence Activities (PPD 28). This training will be relevant to the use of tearlines that include signals intelligence information.

Our submission last year also indicated several areas that we intended to explore in furtherance of our responsibility to provide guidance on producing unclassified cyber products involving identifiable targets. An update tracking our last submission follows below:

- **Data quality:** The IC’s foundational guidance governing production and evaluation of analytic products is Intelligence Community Directive (ICD) 203, “Analytic Standards.” This ICD was re-issued in January 2015, and now includes the requirement that IC elements adopt procedures to prevent, identify and correct errors in PII. In addition, the ICD explicitly reinforces the principle that PII may be included in analytic product only as it relates to a specific analytic purpose (e.g., necessary to understand the foreign intelligence or counterintelligence information or assess its importance).
- **PPD 28:** As we mentioned in our prior submission, Presidential Policy Directive 28: Signals Intelligence Activities (PPD 28) requires certain protections for personal information collected through signals intelligence activities, regardless of nationality. Consistent with PPD 28, all IC elements have published policies that implement those protections. These protections will apply to the extent that personal information from signals intelligence is included in a tearline.
- **Efficacy of ICD 209:** As stated in our last report, the Office of the ODNI National Intelligence Manager for Cyber conducted a study to assess whether ICD 209 provides IC professionals the requisite guidance to produce unclassified reports in a timely manner, including cyber reports that properly use or protect (as the case may be) information pertaining to a specific, identifiable, targeted entity. Feedback indicates that since the data call/study, the elements have worked to refine downgrade processes and handling instructions on disseminated FOUO products to allow them to be shared more broadly. Notably, the study did not produce any directly actionable result nor suggest that ICD 209 is insufficient. Accordingly, ODNI does not plan to revise existing or develop additional policy guidance in this area at this time.
- **CTIIC:** Our prior submission referred to the establishment of the Cyber Threat Intelligence Integration Center (CTIIC) within ODNI. CTIIC was recently authorized with the enactment of the Intelligence Authorization Act for Fiscal Year 2016. ODNI CLPO has assigned a CTIIC Civil Liberties and Privacy Officer to provide civil liberties and privacy guidance to CTIIC personnel. CTIIC’s activities currently focus on providing integrated analytic products to other government agencies. Accordingly, CTIIC personnel receive training regarding rules for disseminating information that contains information identifying or concerning a U.S. person. As stated in our prior submission, ODNI CLPO will assess CTIIC activities to the extent CTIIC becomes involved in activities covered by EO 13636.

2016 EO 13636 Privacy & Civil Liberties Assessment Report

It merits repeating that ODNI as an organization has not historically issued cyber tearlines within the scope of EO 13636, and this remains the case. Accordingly, no audit of ODNI cyber tearline activity has been conducted to ensure that products adequately protect identifiable targets' privacy and civil liberties. Should CTIIC become directly involved with cyber tearline reporting, ODNI CLPO will provide CTIIC with guidance consistent with ICD 203 regarding inclusion of PII in analytic products, and with the training provided regarding PPD 28 (if applicable) and the rules regarding dissemination of U.S. persons information.

Sincerely,

Alexander W. Joel
Civil Liberties Protection Officer
Office of the Director of National Intelligence